Counterintelligence

FORCE PROTECTION
UNIT PROTECTION
AND
COIN

KESHAV MAZUMDAR

)

COUNTERINTELLIGENCE

Now the reason the enlightened prince and the wise general conquer the enemy whenever they move and their achievements surpass those of ordinary men is foreknowledge. What is called "foreknowledge" cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation. Now there are five sorts of secret agents...: native, inside, doubled, expendable and living. When these five types of agents are all working simultaneously and none knows their method of operation, they are the treasure of a sovereign.... He, who is not sage and wise, humane and just, cannot use secret agents. And he who is not delicate and subtle cannot get the truth out of them.... It is essential to seek out enemy agents who have come to conduct espionage against you and to bribe them to serve you.... And therefore only the enlightened sovereign and the worthy general who are able to use the most intelligent people as agents are certain to achieve great things. Secret agents are essential in war; upon them the army relies to make its every move.

Sun Tzu, The Art of War

COUNTERINTELLIGENCE

Intelligence has two objectives:

> First, it provides accurate, timely, and relevant knowledge about the enemy (or potential enemy) and the surrounding environment.

The second intelligence objective is that it assists in protecting friendly forces through counterintelligence. Counterintelligence includes both active and passive measures intended to deny the enemy valuable information about the friendly situation. Counterintelligence also includes activities related to countering hostile espionage, subversion, and terrorism. Counterintelligence directly supports force protection operations by helping the commander deny intelligence to the enemy and plan appropriate security measures.

Stated differently it acts as an early warning system by attempting to provide accurate and timely information about the adversary's intention, and the surrounding environment. It also provides a counterintelligence tool to deny the adversary valuable information and also to combat terrorism, subversion and espionage. Thus intelligence is protective, exploitative and positive in that it supplies us with positive intelligence about the adversary and protects our own infrastructure. Intelligence thus renders our actions either offensive or defensive.

"Intelligence supports the commander's force protection needs by estimating an enemy's intelligence, terrorism, espionage, sabotage, and subversion capabilities as well as recommending countermeasures against those capabilities"

Today's war scenario is of the 4th Generation type. Asymmetry has factored in most battle or tactical operations to a great deal. In fact most of the conflicts around the Globe are asymmetrical in nature , with the players in the combat environment being terrorists, insurgents with very limited firepower , elusive and most of the time operating while mobile , very less identifiable with no conventional forces insignia , very limited personnel strength , distributed and sporadic operational tactics, undefined infrastructure logistical capabilities on one hand and a national power or allies with a formidable military, attack and defense platforms and a central military organization with subordinate headquarters and units spread at unique identifiable geographic locations. Hence not to be subdued by this disparity between themselves and govt. forces the asymmetric adversary

resorts to sudden, sporadic, hit and run type attacks on the forces bases , installations , camps , ordnance depots, communication systems, personnel and information systems with the sole objective to degrade the forces combat capability and kinetic termination of its key leaders at top echelons or middle and ground level tactical units. A kill is a kill. A kinetic hit is a kinetic hit. Whether it's a bazooka attack destroying an armored personnel carriers drive system immobilizing it or whether it's a timed explosion resulting in the destruction of a combat helicopter in the hangar , the end result is the same….we have lost combat capability. In this fashion attacks on our installations,camps,bases,personnel and information systems/communications are designed to degrade our capabilities, exhaust our ordnance on nonexistent targets or dummy targets / proxy targets (deceptive measures of the adversary) –this realm of Threat to our forces itself while in transit or before deployment or in personnel stations and bases and the Govt. forces actions to thwart these threats with intelligence feeds predicating the plans/COAs design is called Force Protection**.**

CI supports Command Force Protection efforts by:

- Identifying the potential threat forces and multidisciplinary threat intelligence
- Identifying threat capabilities and intent together with the most likely course of action and the most dangerous course of action (keeping all the possible COAs parallel for review)
- Using deception to mislead the enemy about our capabilities, vulnerabilities and intentions.

CI & SECURITY REQUIREMENTS:

- Protecting classified information
- Protecting critical resources
- Protecting weapons and weaponry systems
- Safeguarding visitors to the installation
- Protecting dignitaries
- Protecting Senior government officials or military senior stafdf visiting the installation or areas outside the installation but falling within military jurisdiction
- Sustain mission objectives
- Protect information systems

Within the installation thee may be specific person/s,resources,assets,activity,operation or information that if targeted by the enemy can adversely affect the installation operations , mission objectives or any risk dimension—in other words it has ‘’Target value’’ to the adversary. During security planning such entities should be identified (in most cases using red-teaming or counterintelligence support to vulnerability assessment) and secured against enemy actions. Include with this the need to ascertain what adverse effects the local threat can have over the installation as a whole and what missions or contingency plans can be designed to support the installation, and what results is the minimum security requirements in the light of the threat perceived due to the existence of local threat forces.

Local threat assessment usually provides a threat picture specific to a single installation or grouping of installations based on the threat factors mentioned above. This means that each installation may have specific security requirements tailored to its individual assessment.

Resource economy-probably the most important factor in inefficient Force protection

Due to erroneous planning, or improperly defining intelligence requirements or even due to enemy deceptive/denial measures it could very well be that the Commander deploys his resources, combat power and other combat-related assets in the wrong place and time thus exhausting/wasting them and hence resource economy is of prime consideration during any mission and to this end the value of intelligence cannot be overstated. These false responses can be limited and brought down to a minimum by specific, timely and accurate intelligence. Intelligence helps the commander to prioritize his security options. The commander can direct his efforts towards the most important requirements, such as handling the most serious security risks first, mitigate the threat/s which is of lesser severity and accept the inevitable danger and be prepared for risks which are of least severity. Thus the countermeasures will be more appropriately directed against the enemy without any wastage of resources, manpower or lessening in combat effectiveness. All this proper threat driven intelligence and counterintelligence operations, the term ‘’threat-driven’’ assuming greater significance as it then goads the commander to know the unknown aggressively. It should be emphasized that other security agencies should be consulted and information shared with them, both horizontally and vertically to get a complete picture of the threat.

DISTINCTION BETWEEN CI AND HUMINT:

CI Does Not Equal HUMINT

CI and HUMINT , although sharing most of the time similar collection techniques , are not the same thing in the sense that CI is not a subset of HUMINT.HUMINT is an intelligence discipline whereas CI is a multidiscipline function supporting HUMINT.We should not confuse the information collection methods and operational intention. This incorrect doctrinal terminology error will lead to a weakening of both/

HUMINT is solely concerned with collection , not the *purpose of collection of the information* or the requirements which predicate this collection. Yes the HUMINT collector is aware *that the purpose of his collection efforts are geared to collecting information from designated human sources using specific collection techniques. In this sense he is conducting a ‘’pure” collection effort, not concerned with what this information will be used for and what necessitated the collection in the first place.* HUMINT collection includes *“operations conducted using HUMINT collection techniques regardless of the ultimate use of that information.”* HUMINT activities include a great variety of operations, analysis, and liaison duties.

CI on the other hand uses human sources too as source of information but goes few steps further in that CI is aware of the intent of collection and aggressively uses specific techniques to either neutralize or exploit the enemy intelligence activities using the gathered information. Most of the techniques in his repository are similar to that of the HUMINT agent; It is this use of HUMINT skills, particularly investigation and source operations that has created the confusion. CI is a multidiscipline function with the purpose to detect,identify,deter,exploit.neutralize the enemy’s collection efforts—it seeks to counter enemy intelligence geared towards terrorist,subversive,espionage,sabotage or insurgent attacks on our forces and installations and lend support to HUMINT in its activities, protect the intelligence cycle and ensure force protection—a very important factor. Thus we find CI to be composed of several attributes,aggressive,never relenting and protecting the other intelligence disciplines activities(for example , determining whether a source is a source who wants to wittingly give information or is an enemy plant).HUMINT contributes to an all-source visualization of the battlefield , increases the situational awareness of the commander.HUMINT is intelligence derived from persons,documents,a pure intelligence activity whereas CI is somewhat like the hand in darkness..exploring,detecting,getting a hold. Moving ahead with all help that is available in an unknown enemy specific darkness , the enemy lurking in the shadows , whose actions once discerned by the hand will lead to the latter’s firm clasp on his neck.

Hence we must not tend to associate CI solely with HUMINT collection nor define HUMINT in terms of CI.Commanders should understand this.It should not be the prerogative of only intelligence personnel.Commanders,staff officers of operations etc functions should understand this intelligence issue clearly so as to synchronize ops well with intelligence.ISR effort should not be degraded by weaknesses in both HUMINT and CI as a result of this confusion.CI and HUMINT are highly complimentary. Very true but of opposing mindsets.

Conclusion

HUMINT collection and CI are and will continue to become increasingly important as we enter the 21st century. Both efforts are vital to mission success across the entire spectrum of operations. The understanding of the doctrinal distinction between HUMINT collection and CI is fundamental. This distinction drives the doctrinal description of both efforts and our understanding of how they are mutually supportive and intertwined in stability operations and support operations.

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.

Improving Army CI Doctrine

The first step in improving the Army’s ability to collect force protection intelligence is **building appropriate doctrine** that clarifies the role of **Army Intelligence and CI personnel**. Make its information operations doctrine more complete by publishing comprehensive CI doctrine. This doctrine should explain the primary CI missions of collections, investigations, operations, and analysis and production.

Doctrine guides the employment of military forces, and shapes how military professionals “think about the use of the military instrument of national power”. Army doctrine details a basic understanding of the tactics , techniques and procedures to be employed to support combat requirements. Air Force doctrine provides commanders and their staffs a basic understanding of how various Air Force organizations can be used to meet or support combat requirements.

INDIA historically lacked comprehensive CI doctrine.This lack of doctrine has resulted in confusion, and hampered the ability of Force commanders to use CI to improve force protection efforts.

Force protection efforts must be threat driven.Vulnerabilities should be identified , the corresponding threats identified and then protective measures are put in place.To this end MI and CI play a very important role.This should be the basis for the creation of a comprehensive CI doctrine. .

“CI is the systematic acquisition of information concerning espionage, sabotage, insurgency, and related foreign activities conducted for or on behalf of foreign nations, entities, organizations, or persons and that are directed against or threaten our military interests.” To this end a variety of HUMINT sources , like walk ins , casual sources , defectors , official sources , liaison contacts , recruited sources are employed by CI elements. CI collections and investigations lead to a repository of information on threats.Thereafter by cueing other intelligence disciplines and using all source analysis a complete picture of the threat is obtained.Thus we reach our main objective—the precise warning of hostile attack and we also identify the probable targets of the attack and the time of attack.In a nutshell CI usage of HUMINT is the first line of defence.

Army force protection requires a separate force protection doctrine. Not only intelligence personnel will benefit from the doctrine directly but also tactical commanders who must have a basic knowledge about force protection so as to understand what requirements ought to be defined and handed over to the intelligence and counterintelligence personnel to adequately protect the force.

The commanders battlefield operating system at his disposal are fire support and maneuver and here is where intelligence and counterintelligence act as force multipliers –the Intelligence and CI BOS must be successfully integrated in the Commanders BOS so that his PIRs are successfully answered giving him ideally a perfect situational awareness about the battlespace so as to conduct operations successfully. The commander focuses on the intelligence system by clearly designating his priority intelligence requirements (PIR), targeting requirements and priorities. Intelligence is a continuous process which keeps IEW operations tied to the commander's critical decisions and concept of operations. CI collection, analysis, and dissemination, like other intelligence, have to meet the commander's time requirements to be of any use other than historical.

They can then better understand the limitations and capabilities of the CI support elements. Force protection doctrine requires intelligence and counterintelligence personnel to obtain and analyze information on:

- Enemy units
- Terrorist groups
- Insurgent groups
- Enemy special forces
- Criminal enterprises
- Cybercriminals
- Radical elements
- That part of the local populace which supports the enemys ideals
- Environmental/chemical/health/radiological/biological hazards
- Weaponry systems of the enemy units,terrorists,insurgents and crimninal enterprises

Force protection doctrine should compel the creation of Service capabilities to collect, receive, evaluate, analyze, and disseminate all information on terrorist activities,strength,capabilities,organization,intent,past history, current activities in the area in question or areas of interest and indicators of imminent attack.

We can categorize the threats based on intent. This can be incorporated in the force protection doctrine. Hence we can allocate HUMINT resources in an appropriate manner without any duplication or wastage. Type 1 can be criminal activity geared towards army bases ,Type 2 can be penetrative reconnaissance and sabotage operations, terrorist and insurgent attacks , and Type 3 can be major land , amphibious , air and missile attacks.

TYPE1, 2 and 3 threats can be adequately determined by the employment of counterintelligence assets which use HUMINT sources to collect force e protection information and conduct investigations , security surveys ,threat and vulnerability assessments. Casual sources, official sources, liaison contacts and recruited sources comprise the source database of the CI repository. All source intelligence is also used for all the threats, particularly TYPE4.These include HUMINT, SIGINT.MASINT, IMINT, ELINT AND OSINT.Fusion of all information from multidisciplinary intelligence platforms with data from national level intelligence agencies result in far better situational understanding of the Commander. ISR synchronization is a must if we have to have a robust advance warning system to avoid the element of surprise.

We can make certain observations after studying force protection failures from around the globe:

- HUMINT was not given priority in force protection efforts , neither the HUMINT support was precise, effective and tailored to the Commanders needs. Instead standard operating procedures detailing standard and routine defensive methods and access control were implemented.HUMINTs capability in predicting on how , where and when a terrorist attack might take place was ignored.HUMINT can predict the specific target ,time and nature of attacks.

- Lack of organic intelligence capability at tactical level.. “They did not have a **dedicated, organic, and focused [force protection] intelligence analytical capability.”Plus there is a weakness in both collection and analysis of force e protection intelligence.** If intelligence capability can be pushed down to company/platoon level with the soldiers being augmented with 2-3 HUMINT and 1-2 CI operatives (or the soldiers themselves being trained in the basics like tactical questioning and interrogation) then instead of sending request for information to higher headquarters the tactical capability to investigate , gather information and analyze it would have been achieved. The ‘’always top-down’’’ intelligence flow could have been avoided and a four way flow implemented with interaction between the tactical units and higher headquarters, adjacent company headquarters and intelligence elements.Hence there is a **desperate need for military units operating in high-threat environments to possess organic intelligence collection, analysis, and investigative capabilities.**

- Military intelligence lacked the necessary impetus to devote time, effort and resources for long-term and mid-term terrorist threat intelligence collection and analysis – such as trends, intentions and capabilities of terrorists. National intelligence agencies were larger in operational and administrative size and were given priority rather than the MI in collecting intelligence but national level agencies cater to a wide range of requests for information apart from terrorist threat to forces whereas MI can exclusively set up collection taskings for force protection intelligence given adequate weight age , administrative and financial aid and clearance by the Government. This was absent.

- The installation in question fell prey to terrorist attacks because the intelligence arrangement at Command level in higher headquarters or at the installation headquarters itself was focused on outward attacks like tactical missions, or defensive postures dictated by air

threat and totally ignored the need for HUMINT/CI based intelligence collection for ground defense of the installation, personnel, information and communication facilities.

To execute a CI operation successfully liaison is needed with other civil agencies and with the intelligence agencies of the 3 services.To effectively build up a liaison time is required,it cannot be achieved overnight.In case of COIN operations liaison is much needed with the local administrations intelligence branch and with the police as they are the ones who know the local area,population,criminal elements and insurgency profile in terms of attack history, police records of personalities and elements who have been apprehended and surrendered..the latter can be put to use by the counterinsurgents as pseudo-insurgents to penetrate the adversary's setup. Liaison relationships are an investment in the future, and the return on this investment is directly proportional to the time and effort expended on developing and maintaining the relationship.
We can transfer say 2-3% personnel from the MI to the CI unit as CI units are generally understaffed compared to the standard HUMINT units , and the liaison units. Even transferring 3% personnel can significantly raise the strength of all the units overall. Thus with this transfer the Commands HUMINT assets get a boost and now coupled with CI augmentation the HUMINT teams can handle all three types of threats , Basic , Levels 1&2.
Simply transferring will not suffice, proper training in counterintelligence need to be given. But this wont be a problem as the MI soldier already has basic intelligence training and acumen. Yes they need to be granted clearance to access compartmentalized intelligence information and hence prior to transfer the soldiers need to undergo a counterintelligence investigation process as to their suitability.

The CI effort focuses on the overall hostile intelligence collection, sabotage, terrorist, and subversive threat. The CI effort is also sufficiently flexible to adapt to the geographical environment, attitudes of the indigenous population, mission of the supported command, and changing emphasis by hostile intelligence, sabotage, terrorist, and subversive organizations.

What Are We Protecting?

In protecting an installation and its information systems, operations and general security from enemy multidisciplinary intelligence threat we must identify the vulnerable and critical areas to be given more weightage during security review. Not all assets and activities warrant the same level of protection. To this end a careful and thorough vulnerability analysis needs to be conducted resorting to red teaming methodology.

It should be noted at this juncture that it is always the attempts of the enemy intelligence service to subvert our knowledgeable personnel. In a military production unit , say ordnance factory , the senior engineers and quality control scientists have access to sensitive designs and information related to weaponry systems. Similarly classified and top secret documents/information are in the hands of cleared senior personnel. These people are often the target of aggressive enemy counterintelligence agents.

The five basic categories include the following:

1. People
2. Military personnel
3. Activities/Operations
4. Intelligence collection/analysis
5. Sensitive movement of operations/personnel
6. Conduct of sensitive training
7. Communications/networking
8. RDT&E and sensitive technology
9. Production of sensitive technology
10. Protection of nuclear/chemical/biological materials
11. Protection of weapons, explosives, and equipment
12. Information
13. Classified
14. Sensitive Compartmented Information
15. Top Secret
16. Secret
17. Confidential
18. Unclassified
19. System designs
20. System capabilities/vulnerabilities
21. Sensitive methods
22. Facilities
23. Headquarters

24. Field offices/administrative buildings
25. Training facilities
26. Storage facilities
27. Production facilities
28. R&D laboratories
29. Power plants
30. Parking facilities
31. Aircraft hangars
32. Residences
33. Equipment/Materials
34. Transportation equipment/vehicles
35. Maintenance equipment
36. Operational equipment
37. Communications equipment
38. Security equipment
39. Weapons
40. Automated information systems equipment

Now that the CI agent is knowledgeable about these assets and activities that need protection, he can execute a vulnerability and criticality analysis and recommend suitable protective measures as well as countermeasures to the Commander. He can recommend which critical units need protection first and what resources to allocate and how and where to implement general security and countermeasures.

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
- Asses 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*

The above factors are contained in the Detect-Assess-Decide system."(DAD).

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 passive 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 to base our decisions regarding collection of intelligence , fortifying and strengthening/hardening our bases, decide on the optimum courses of actions , 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 protective 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 tactical operations’’ ..not just tactical operations. Protection should be a 360 degrees hemispherical capability , meaning protection from land , air and sea based attacks.

For protection intelligence is critical as everything needs to be known about the enemy , environment and self. The last factor is determined by counterintelligence reviews , technical experts and red teaming.All intelligence platforms and ops must be thoroughly integrated to handle attacks fro m land , air, information , electronic,CBRNE,and intelligence domains of the enemy. This integrated approach heightens the commander’s situational awareness considerably , thus acting as a force e and decision-superiority enabler thus leading to optimum effective course of action/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 unnecessarily 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 cooperation's 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.

Unit protection must integrate the protective attributes of different Army Corps. The capabilities in brief of the Corps are as follows:

- 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.

- Military Police provides security by executing proactive intelligence led policing.

- 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.

- Military intelligence provides security to our force by adequate synchronized utilization/deployment of ISR assets and counterintelligence capability

- Signals protects our command and control nodes directing/controlling communiucation,computers,and intelligence operations. Siugnals intelligence directly supports HUMINT operations to validate information,increase the situational understanding oif the Commander.

- Field Artillery provides security to the force by contributing to the direct/indirect firepower,predicting impact points.

- Ordnance Corp contributes to recovery by deploying its ordnance disposal systems.

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 entire range of hostile activity including intelligence collection and counterintelligence activities, use this information to assess its capabilities and 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 more accurately, 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.

ACTIVE MEASURES FOR UNIT PROTECTION:

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.

From the force protection perspective CI and 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

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 disseminatin.

Warning is of two types:

(a) Defensive warn

(b) 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:

- It should allow for redundancies in our act capability systems.
- 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.
- It should provide a system of integrating fires to handle threats and precluding enemy attack on our installation , its C2 and critical assets.
- Provide warning of threat intelligence activities.
- Provide warning of existing threat C2 nodes
- Provide warning of threat capabilities, disposition, strength, order of battle
- Provide warning of threat logistic routes.
- Provide warning of threat sympathizers.,
- Provide warning of threats possible attack COAs
- Provide warning of the defense capability of the threat
- Provide warning of threats peculiar /preferred TTPs/modus operandi
- Provide warning of threats history
- Provide warning of threat movements
- Provide warning of threat leadership
- Provide warning of threat detachments, cells dispersed in and out of the area of operations.
- Provide warning of Threat attack /defense operations location parameters.
- Provide warning of potential attack/defense methods of threat.
- Provide warning of the expected time of attack.
- Provide warning of possible locations of Threat listening post/observation posts
- Provide warning of possible escape routes of threat forces after an attack or defense scenario
- Provide warning of possible enemy IED techniques, infiltration routes, emplacement
- Provide warning of IED detonation methods/means
- Provide warning of IED timings
- Provide warning of possible routes for IED ex-filtration
- Provide warning of Staging areas
- Provide warning of Safe houses
- Provide warning of weapons and ammunitions storage locations

- Provide warning g of the Production facilities for IED and other ammunitions/explosives.
- Provide warning of supplementary operations threat may resort to
- Provide warning of threat indirect fire parameters, key indirect fire

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?

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.

CI and COIN

Why does counterintelligence factor so much in COIN missions? Firstly insurgents place a very high emphasis on the usage of informants, double agents, reconnaissance, surveillance, open source collection of media and imagery. Thus it could well be that we have sources who have switched loyalties or who may be working for both the parties with little or no loyalty to the government. We must locate these individuals who are a threat to operational

security.

Secondly insurgents resort to countersurveillance.They hide among the local populace , use couriers to transfer money , intelligence and orders to run their ops.

Finally and very important is the need for counterintelligence for Force protection.
Another definition is CI both ‘information gathered’ and ‘activities conducted’ in order to ‘protect against espionage, other intelligence activities, sabotage or assassination conducted on behalf of foreign powers, organizations or persons, or international insurgent activities but not including personnel, physical documents or communications security’. In order to neutralize hostile intent CI conducts various activities such as acquiring information about plans , operations and capabilities of those organizations whose intent is subversion.CI informs policy. It aids military commanders and allied agency heads to take effective decisions. We don’t have a clear doctrine on CI.It is the most misunderstood , most sensitive arcane intelligence discipline.But it performs the very important function of protecting the intelligence cycle.

Counterintelligence is both an activity and its product. The product is reliable timely information about enemy/foreign intelligence organizational structure , the personnel profile , the operations of the enemy/foreign intelligence service and how they recruit personnel both from outside and insiders.To this end ‘’counterintelligence intelligence collection’’ activities are conducted.It is an organization too as it consists of personnel with specialized skills to whom are allocated various functions , which after proper

execution an information database is created which provides knowledge to decision makers.

Summing up CI is in a way different from all other intelligence disciplines.*Intelligence seeks to acquire information through collection methods wherein the result is not the objective but in CI collection activities enemy intent is always in the horizon..and activities..both offensive and defensive are conducted to neutralize this intent or to exploit the enemy itself to our advantage.*Counterintelligence interacts with other intelligence disciplines such as SIGINT and IMINT to locate hostile entities and also to acquire knowledge about the capabilities and targeting of hostile SIGINT/IMINT.CI is multidisciplinary.It is different from security in that like security it does not only seek to implement defensive measures but also to aggressively target hostile intent.One of these offensive CI operations is Deception.Deception ops are designed at senior echelon levels such as Command. The CI body/unit executes the deception operation. Just as tactical military intelligence supports combat ops , similarly CI must support deception ops.CI is not policing.Once a crime is committed the law enforcement authorities resort to arrest of the perpetrator so as to prosecute him as per law. But a CI agent has no arrest authorities. All these doctrinal differences make it more difficult to promulgate a clear CI doctrine.

The CI functions include collection of all information about the activities and the organization itself of the enemy intelligence service. To this end source operations and clandestine methods are resorted to. The analytical component of CI holds significant importance because accurate analysis predicates CI operations designed to defeat hostile intent and also conduct exploitation ops to our advantage .Infiltration/penetration and deception operations , to name a few are the offensive operations resorted to by the CI body. A specialized function is the evaluation of defectors and debriefing of returned defectors. There are also defensive operations designed to protect installations/personnel/information and formal security programmes.

Protecting secrets -- High up on its priority list CI has information protection.CI attempts to ensure that classified information doesn't fall into the hands of unauthorized users such as foreign agents /foreign intelligence service (physical security part of CI) and also making certain that all those people who do have access to sensitive information , say due to ''need to know'' authority or by virtue of portfolio in the intelligence deptt.—these people are protecting that information from being accessed. Here I used the term "CI attempts to ensure'' as no amount of security controls can ever guarantee that the employee will observe the rules. Lapses will and do happen. Lapses which may be involuntary or voluntary with multiple intent scenarios ..ranging from yearning for self sufficiency in terms of wealth etc to disgruntled officials. If an official has the authorization to access sensitive information we must accept the fact that the information can also be compromised. To prevent this from happening and thus protect the intelligence information (or in a larger context the intelligence cycle itself) the intelligence organization resorts to psychological/behavioral evaluation/monitoring and profiling those personnel who have a propensity for betrayal. But the former evaluation techniques are below 100% accuracy thus leading to the recruitment of personnel who have intent to do harm. As for the latter profiling method those personnel who are adept in evading detection remain out of scrutiny and more resources are wastefully allocated in profiling the wrong person. Hence I had earlier stated that no amount of security control or vetting can ensure 100% information protection. We have to live with this risk and CI primary function is to resort to all available means so as to minimize this risk.

Counterintelligence force protection source operations

Attacks against military and related facilities are a very real threat, as demonstrated by the Naxalite attack against CRPF personnel in Chattisgarh's Dantewada district and many others. On April 6, Naxalites had killed 75 CRPF personnel and a police officer also succumbed in the massacre.We must have a doctrine for protecting our facilities and conserving the potential of our forces.Insurgents deliberately attack the forces ..for example in the rear to destroy camps,housing,support units and ammunition dumps with the intent to undermine the fighting potential and morale of the troops and loot and destroy its ordnance and weapons simultaneously.This is a grave threat and needs to be addressed.

Counterintelligence , like it protects the intelligence services it also provides the necessary intelligence to combatant commanders for force protection.Standard intelligence disciplines all provide relevant intelligence but very less or no HUMINT relevant to counterintelligence.

Yes we incorporate standard physical security measures but that is not sufficient for force protection.It is never a substitute for protection gained through intelligence.Moreover physical security can never override the value of counterintelligence.It is only HUMINT collected by intelligence and counterintelligence agencies that function as the indications and warning provider with respect to insurgent and other force protection threats.

CI is indispensable in COIN operations where it is practically not possible to employ ground warfare tactics as against a conventional enemy.What is required here is a severe dampening of the morale of the insurgents and render their efforts ineffective.CI can assist in projecting a ‘’threat capability’’ far superior to that of the insurgents.By the term ‘’threat capability’’ we are singling out the ;;threat’’ component of the force instead of focusing on our forces itself—threat of force.This is a psychological application of out ‘’force’’ capability and if properly applied can go a long way in winning a war where only killing the insurgents is not and can never be a solution.

Database:

COIN operations should not only focus on the insurgents but also on other criminal elements which have been known to abet the insurgents , the relationship being predicated by the satisfaction of each others needs.We need to focus on terrorists,drug mafias and any foreign intelligence service which supports the insurgency.Political , economic , social,geographic,demographic and military conditions existing in both the area of operations and the larger area of interest needs to be considered.All these information need to be compiled , indexed and recorded in databases , updated regularly for retrieval when the need arises.The database must also be supported by a source registry to avoid conflict.The database provides a framework on which to base threat assessments, vulnerability y assessments and force/unit protection counter-measures.

Threat Assessment

We need to determine precisely the intent,capabilities,activities,leadership and C2 nodes,table of organization and equipment,doctrine,observed tactics , techniques and procedures ,ideology, internal/external support,logistics,HUMINT,SIGINT and IMINT activities/capabilities,CI,communications,and other methods of operation of the insurgents in order to prepare a thorough threat assessment report. Special focus should be on:

- Intelligence collection.
- Espionage.
- Subversion.
- Sabotage.
- Terrorism.

The threat assessment should be a complete picture , in its entirety meaning nothing should be left out , including other criminal enterprises and foreign intelligence collection and support activities operating in the area.

This threat assessment will be one of the most important tools for the Commander in the planning phase as it will lay before him the information gaps—information which needs to be known, translated into intelligence requirements. The Intelligence staff officer will continuously update him on all happenings in the AO during the planning phase and the operations officer and the former will work hand in hand , in fact in a totally integrated fashion , each taking cognizance of the others capabilities, constraints and methods of operation. The operations officer assists the Commander in detailing all the possible courses of action as against enemy courses of action , all the while keeping in mind the intelligence collection assets available to him and their limitations while the intelligence officer will attempt to understand the intelligence requirements of the operations officer precisely so as to deploy his assets optimally, keeping in mind the availability constraints, type of platform and priority of the requirement—the last factor being very important.

As such Source Operations are conducted by the counterintelligence units and casual or incidental sources such as listed below are screened and debriefed/interrogated:

- Walk-ins and write-ins (individuals who volunteer information)
- Unwitting sources (any individual providing useful information to counterintelligence, who in the process of divulging such information may not know they are aiding an investigation)
- Defectors and enemy prisoners of war (EPW)
- Interviewees (individuals contacted in the course of an investigation)
- Official liaison sources.

Active and Passive protection Measures. The application of active and passive measures resists adversary plans and actions directed against friendly personnel, assets, and information. The utilization of the act function and its related protection capabilities enable a commander to preserve operational capabilities via the improved protection of personnel, assets, and information.

- Active Measures. Active measures include the ability to deter, prevent, and deny adversary plans and actions, to include offensive actions.
- These offensive actions may take the form of preemptive and direct attack against enemy C2 nodes, assembly areas, weapon caches, AMD, and computer network attack (CNA).

- Passive measures. Passive measures and reactive protection include the ability to deter, prevent, and deny adversary plans and actions from using a capability the enemy would otherwise employ against the JF.
- These measures provide the capability to defend against adversary actions once those actions are executed or when friendly forces are confident the adversary will imminently use adverse actions.
- These measures may include specific types of camouflage; cover for supplies and personnel during a NBC attack or the utilization of bunkers during RAM attack.

Physical Security

Physical security SOPs and other ramifications of protection of physical assets is predicated by the need of protecting military installations/bases,personnel,operations and other activities from foreign intelligence threat and terrorists, subversive agents, insurgents and saboteurs. The staff officer (Ops) and the Provost Marshall look after the perimeter security aspects while the CI personnel conduct security reviews and recommend safe practices, security controls and procedures for all threat scenarios possible.

The perimeter affords the minimum defensive measures and should be so constructed so as too exert maximum possible access control and least opportunities of getting breached. To effect this the following should be given particular note:

Squads should patrol for effective reconnaissance and surveillance. Such R&S measures serve as deterrence against possible terrorist or insurgent attacks by breaching perimeter defenses. Detection and deterrence are the two main functions of R&S teams patrolling the perimeter and adjoining external areas. Tactical equipment like radars for ground surveillance, remote sensors should be emplaced.

Restricted areas should be clearly marked , but as against conventional large letter red markings which can attract attention and apprise the enemy about the sensitiveness and importance of the marked area thus placing it in his attack plan , area can be divided into zones or quadrants , each bearing a color code as per its importance relative to the entire installation and these color codes can be placed on authorized entry/work permits for civilian hires/staff so that they do not access other quadrants. Moreover each civilian should be tagged and given a daily entry pass (with date and time fields for say one month entry and photograph and personal identification fields)which

should be returned at the main military police entry point on leaving the area. The gate pass submitted at night must be the same pass to be issued to the civilian employee next day at time of entry. If the pass was not submitted at night time with the time recorded on it at submission, it is not valid and the civilian will not be readmitted and will be taken into custody for questioning as to why the pass was not submitted. This pass system may incorporate quadrant color system for heightened security.

Every visitor and employee should be thoroughly checked for weapons and explosives, female staff being used to conduct searches on the female entrants. On exit again a thorough search should be conducted to deny the civilian or visitor any opportunity of theft. It is a wise idea to ask the local police station to augment the military police with few of their personnel to conduct searches as police searching a civilian is much less a problem than a military person frisking the subject which most might consider offensive. Military personnel should also be subjected to searches for concealed weapons or explosives if 100% security is envisioned. All civilian vehicles can carry explosives properly emplaced and out of normal sight, such vehicles should be searched thoroughly. There have been cases when the tyre portion was cut off and explosives inserted and the tyre again retreaded.The sniffer dogs fail to detect the explosives due to the tyre retreading odour.Hence tyres and everything which is felt does not have any capacity to conceal an explosive should also be checked.

Remember that if POL/Ammunition dumps are co-located with the perimeter then a well placed charged can blow up everything instead of single targets. The terrorist will find this an easier way to inflict heavy damage to the installation. Moreover if the perimeter is severely damaged and in the resultant chaos everything goes out of hand the enemy can now move in to inflict further damage. Hence ammunition storage areas and POL should be located within the containment area but away from the perimeter and hospital , personnel barracks and also the command post/tactical operations center.

The entire restricted area quadrants should be so divided so as to restrict the government of civilian personnel and hires as close to their authorized quadrants as possible and minimum passes by the other restricted quadrants. Bug and other electronic spy ware devices should be periodically checked by technical sweeps. The color codes should be periodically and randomly changed. A guard system should be in place for each quadrant to monitor the civilians, the guards being both mobile and stationary. All these areas should be off limits to all but
Authorized personnel and must be marked as *Restricted Areas.*

Designate all sensitive areas of the installation as
Restricted areas. *Restricted areas include:*

- Intelligence offices and barracks
- Ammunition storage areas
- POL
- Command Post
- Tactical operations control center
- Communication systems

One should take note of the fact that if obsolete or unserviceable military equipment, communication systems , weaponry and small arms are not destroyed or evacuated they can fall in the wrong hands and

transformed into IED and booby traps and mines by utilizing the parts/ high explosive chemicals and a germ of an innovative idea. Cans, brass cartridge
casings, and dead batteries have been used as mines,
booby traps, and detonators.

Individual activity or movement profilers should be randomly changed. For example the commandant should not use the same route or same timings for his trip home or to another base. Established patters make it easier for terrorists and insurgents to destroy their target. It is a good idea not to exhibit rank and position associated with high profile military officers by wearing uniform always outside the military secure area.OPSEC should be followed closely and no loose talk should happen with any civilian, however trusted, inside or outside the base. Operational profiles should also include the random element.POL trucks should not go for refueling at the same time each day—there can be ambush points enroute , the vehicle taken over and now the terrorist/insurgent drives straight into the fuel dump with the truck containing his planted explosive.Staging,training and planning of military operations should be subjected to randomness. **All security measures should be viewed and undertaken with the knowledge that there is no rear area in counterinsurgency. Rather, you have a 360-degree dispersed battlefield.**

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 are designed.Personnel,physical and information—these three are critical assets and need to be fully secured against multidimensional threat intelligence collection efforts. Security education and training is inducted in the force with exactly this intent. The focus is primarily on the multidimensional threat intelligence collection efforts, the espionage threat and overall security threat factors. The soldier's awareness is heightened in these fields. The concept of insider-threat is also a major area of study.Terroism and insurgency is also dealt with. 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.

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.

TACTICAL OPERATIONS

Counterintelligence support to tactical operations take the form of cordon and search operations. Cordon and search operations are conducted to locate ,identify and detain hostile elements who are taking shelter in a community or a specified area. These elements take sanctuary with the intent to cloak themselves in a fabric of the otherwise harmless ''local'' and also to use the community or area as a support base. Cordon and search operations also yield information and tactical intelligence upon questioning the detainees.

- Cordon operations require planning , that is if time permits.The tactical unit commander must have a thorougfh knowledge about the key terrain,the local community and should make it a point to keep defectors , turned-insurgents,informers and other people who can help in the identification of the insurgents and their affiliates/supporters from within the locals within the security perimeter enforced by the cordon.CI elements should be accompanied by trained HUMINT interrogators and PSYOPS personnel.Cordon operations usually take place at night and search at first light but if situations warrant the ops at daytime then the tactical commander should take adequate preparations not to alert neighbouring locales.It should be remembered cordon and search operations unmask the insurgent infrastructure if carried out properly.This is a very important tactical operation.The task of the CI support staff is to:

- Assist the tactical commander during tactical questioning
- Keeping up-to-date the intelligence on the local community and area
- Coordinating with the tactical unit commander so that the ops is conducted smoothly
- Update existing black or grey lists. This also means helping in kinetic/non-kinetic targeting after intelligence is retrieved on questioning the detainees.

Community Operations

In the basic cordon and search operation there is the screening element , the search element and the sweep element. The screening element sets up a center for collection ,the search element follows behind the sweep element searching for those persons who hold information of value, and also look for evidence such as weapon cache,radios,documents,maps ,communication codes etc while the sweep element escorts these persons to the collection center for screening. The search element comprises two teams , one consisting of CI personnel and the other interrogators. Prior to the operation these personnel are handed over the list of persons who will be of interest to the counterintelligence team.

The holding station or collection center is made up of different categorized screening stations , say one of informers, one of cooperating prisoners, the other the community head while another could be enemy defectors. The enemy defectors and the cooperating prisoners may be hidden from view and will assist in identifying enemy personnel and sympathizers who are mingling with the community.

Properly segregating those identified persons is very important.Therafter the interrogators take over. Keep in mind to cross check the profiles of identified and segregated persons with that of the black list. Ask for identification papers., match the photographs (if available) with the persons. Those whose photograph is not there immediately take their photos. Set up a second phase of interrogation by a different interrogator team and cross check the statements extracted with those that were divulged before the first interrogator team. If you still feel that certain persons can divulger more information of counterintelligence interest dispatch them to a marked detention area from where they are transported to cells where further interrogation can be executed. Be alert for persons who may attempt to escape or break through the cordon and detain them. Once all threat elements have been identified dispatch the innocent members of the community to their homes and transport the threat elements to base for further interrogation.

The Cordon and Search operation involving large areas is quite different and personnel-intensive in that apart from a large military force and sufficient HUMINT/CI personnel and other intelligence

resources to cover the area , also required is the local police , paramilitaries and communication and logistical systems on a large scale. The sweep and search elements conduct screening operations inside the perimeter of the area which is systematically subjected to the operation community by community , and as search progresses the military force outside the perimeter keeps a constant vigil to intercept escapees , intruders or people with avoidance tendency. The people of the community who have been screened will be issued passes which will testify to that factor and allow them travel relaxations , of course never outside the area. It is very important to observe OPSEC procedures and restricting information flow only between the participants of the C&S operation , as such operations are large in scale , may take days and hence are easily detected by the enemy who will do everything in its power to impede the progress or effectively nullify the operation. The CI team who will conduct interrogations of those screened persons who may offer information of intelligence value but need interrogation , are collocated with the tactical C&S headquarters centrally in the area. The interrogation centre will also be manned by police interrogators and interrogators from other agencies. It is here that the screened persons with intelligence information are escorted and subjected to interrogation. One should remember that enemy intelligence can have plants in the screened persons.Whatever be the case systematic interrogation will reveal intelligence of interest to the CI personnel which can be exploited further ,Going further , there should be a quick reaction tactical team to act immediately when the extracted intelligence is perishable (very time sensitive).

FORCE PROTECTION PROBLEM

CI SUPPORT TO FORCE PROTECTION

NEWS CLIPPINGS:

Kashmir attacks: Indian troops killed

INCIDENT 1 : Security forces in Indian-administered Kashmir say they have shot dead three men who stormed a police station and an army camp, killing at least 10 people. The gunmen were wearing Indian army uniforms when the attacked the station in Kathua district and the base in Samba district, said police.

Kashmir has seen an armed insurgency against Indian rule since 1989.

Indian Prime Minister Manmohan Singh described the attack as barbaric, but said it would not derail peace efforts.

He is due to meet his Pakistani counterpart, Nawaz Sharif, on the sidelines of the UN General Assembly this week.

Peace talks between the two countries have been stalled for the past two years, and dialogue is expected to ease recent tensions along the Line of Control that divides Kashmir between the two countries.

India has a large security presence in Kashmir with tens of thousands of police and paramilitary forces deployed in the region.

On Thursday morning the attackers, dressed in army uniforms, arrived at a police station in Hiranagar in Kathua and opened fire.

Four policemen and two civilians were killed in the attack, police said.

The militants then hijacked a truck and fled, senior Kashmir police official Rajesh Kumar told Reuters news agency.

"They abandoned the truck on the national highway and perhaps took another vehicle and carried out an attack on the army camp in Samba," he said.

“Militants early this morning attacked the Mesar camp of 82 armored regiment in Samba district. They are using grenades and automatic gunfire to carry out the attack. Most likely, two militants are involved in the attack,” a senior police officer told IANS.
The Army camp houses 82 armored regiment which comes under the command of Army's 9th Corps that is headquartered in Yule Camp (Dharmshala) in Himachal Pradesh.

The same camp was also attacked on September 26, 2013 by militants after they had attacked the Hiranagar police station in Kathua district. Twelve people had been killed in that attack.

Today's militant attack came on the morning of the start of the nine-day Navratri festival, and on a day when Muslims are celebrating Nowruz, or the Persian New Year, in the state.

Just yesterday, six people including two militants were killed in a similar attack on the Rajbagh police station in Kathua district. Intelligence reports had indicated that four militants were involved in Friday's attack, but only two had been killed.

Intelligence sources said that they believe the Saturday's attack is being carried out by the two guerrillas who survived in yesterday's attack after escaping from the spot.

REPITITION? The Mesar camp was also attacked on September 26, 2013 by militants after they had attacked the Hiranagar police station in Kathua district. Twelve people had been killed in that attack. On Friday, six people including two militants were killed in a similar attack on the Rajbagh police station in Kathua district.

INCIDENT 2 : Jammu: A civilian and three security personnel were killed on Friday when two heavily-armed militants stormed a police station in Jammu and Kashmir before being gunned down, police said.
The attackers were killed over seven hours after they barged into the Rajbagh police station complex in Kathua district after gunning down the lone guard at the main gate, police officials said.
Armed with automatic weapons and grenades, the militants, dressed in military fatigue, carried out the sudden attack at around 6 a.m.
Once the attackers sneaked into the complex, about 65 km from Jammu on the highway to Pathankot and just 15 km from the Pakistan border, they opened fire at a building occupied by the Central Reserve Police Force (CRPF), killing two of its men.
A civilian was also killed but it was not clear in what circumstances. Ten others, almost all of them security personnel, suffered varying injuries in the audacious attack.
Inspector General of Police Danish Rana announced the death of the two militants. The others dead were a policeman, two CRPF personnel and a civilian.
The injured included seven CRPF men, a deputy superintendent of police, a police constable and a civilian, Rana added.

INCIDENT 3 : 300 rebels initially attacked a convoy of the paramilitary Central Reserve Police Force (CRPF) in the Talmetla area as they were returning from an operation. India's home minister P Chidambaram said that it appeared that the forces had "walked" into a rebel ambush by returning to the police base via the same route they had come. "Something has gone very wrong. They seem to have walked into a trap set by the [Maoists] and casualties are quite high," he said. Police sources reported that the Maoists triggered two land mines targeting the mine protected vehicles carrying the jawans. The attack took place when the CRPF unit belonging to the 62 Battalion entered the forest for an operation between 6 and 7 am and were ambushed by the Maoists.

The Threat.

The threat, the adversary must be known as much as possible for successful CI operations. A thorough analysis of threat and its capabilities is very necessary. The adversary conducts multidimensional intelligence activities and its doctrine dictates that to be successful it should be aggressive, conducting its reconnaissance operations actively and continuously under every set of conditions and that continuity, timeliness and accuracy is essential

Adversary may use HUMINT, IMINT, SIGINT AND OTHER INTELLIGENCE DISCIPLINES operated through a variety of collection platforms and to counter this tactical or strategic threat, as the case may be, we must have a comprehensive CI program in place. The adversary uses multisensor collection means to offset our attempts of countermeasure and deception.

The foreign intelligence service conducts intelligence collection about our forces and hostile attack. Herein comes the very important concept of force protection. They target defense personnel , resources , activities and critical information.CI support to force protection involves actions to prevent or mitigate hostile actions against these entities.It should be noted that the military police functions are not adequate to cover the security of these entities –CI support is a must.In a deployable situation the enemy targets the vulnerable rear positions and the support elements.Hence security is beefed up where troops are housed , dependants and other personnel are made aware of the threat—this is where the CI elements are active..

The military police and allied elements take stock of the situation in the army area but are less aware of the ground situation ‘’outside the fence’’.Hence recourse is made to establish contact with civil intelligence agencies and local police for updates on any threat intelligence in the proximity of the base. Moreover the military police have no jurisdiction outside the base. Strengthening the physical defenses is one way to prevent the application of hostile intent but what is more important is enemy pre-operational surveillance activities. But the difficulty is that these activities are innocuous.

Let’s take an example to illustrate the point. A vehicle approaches the gate of a military camp. On being questioned by the guard on duty the driver says he had no intention to turn up there—he had made a wrong turn. Now this is an acceptable excuse and further interrogation may not help. The driver is instructed to leave the area.Fine.It is equally possible he is saying the truth. But consider the situation where the the threat index in the area is high and hence from the force protection perspective the driver who can equally well be a insurgent has just conducted successfully a preoperational surveillance. There are options. The license details of the driver can be jotted down. The car details and license plate number can be taken. Offhand queries can be made. A listing can be made of all ‘’lost motorists’’. The information can be shared with the local police. If it is found out the same driver has turned up at other installations with the same story , well we have a case of pre-operational surveillance and with the jotted information in hand steps can be taken. But still the case is rare as there are several instances of genuine lost motorists.

Whatever any installation together with its constituent personnel , their dependants , operations and information is susceptible to hostile attack and intelligence collection.CI elements must shield the installation from such intent by guarding the rear and vulnerable areas.CI should lend support to mobilization security , major records repositories , anti and counterinsurgency operations , rear operations , psychological operations , battlefield deception , operations security and CSIGINT.

We can categorize the threats based on intent. This can be incorporated in the force protection doctrine. Hence we can allocate HUMINT resources in an appropriate manner without any duplication or wastage. Type 1 can be criminal activity geared towards army bases ,Type 2 can be penetrative reconnaissance and sabotage operations , and Type 3 can be major land , amphibious , air and missile attacks. Thus commanders can tailor defensive actions compatible with the type of attack. Mission of CI can be clearly defined , objectives stated and qualitative/quantitative protocols in collection efforts underscored. Keeping each type of attack in perspective and with the notion of CI as ‘’looking inwards’’ in mind we can identify the critical areas of installations, and implement security measures. At the same time we can launch aggressive CI operations to frustrate enemy intelligence collection efforts.

It is true that a multidisciplinary intelligence approach is effective to thwart enemy collection efforts but CI and force security measures play key roles. To neutralize/destroy enemy intent we need CI to the fullest capacity. Other intelligence disciplines can be cued but CI is top priority. To identify our vulnerabilities we must resort to counterintelligence. Intelligence is looking outward but CI is looking inward. Intelligence collection is not concerned with the end result but counterintelligence is concerned with the ‘’intent’’ of collection.CI should always be on an aggressive footing. We need a comprehensive CI doctrine detailing all of these and more.

We should bear in mind that this era is not exclusively the era of conventional combat. Asymmetric warfare is the order of the day. Insurgents take years to plan an operation. They conduct extensive pre-operation surveillance , they have their own counterintelligence networks and this long period justifies the employment of intelligence and CI .

The CI department should tackle the type 1 , 2 and 3 threats.CI cells should come into existence and should be staffed with HUMINT , SIGINT and IMINT elements. Priority should be on analysis of threat intelligence.MI should be particularly in charge of analysis of Type 3 threats.Elements from Special task forces , explosive ordnance disposal, medical , operations and communications should also staff the CI cells. The CI elements should fortify their collection and investigation capabilities. They should maintain a threat database which will include the structure and capabilities of foreign intelligence services , details of insurgent organizations and timeline of attacks perpetrated by them and also criminal enterprises because it is well established that insurgents and criminals share information and resources. This database should be continually updated. The intelligence information contained in this database should be readily available on request. Included in this database should be latest physical security measures , details of explosive ordnance effects—all contributed by specialists. All source intelligence should be further fused in with the intelligence contained in the database.

The CI analytical cell should not only produce daily threat summaries but also act as and I&W system. It should receive worldwide inputs of insurgent developments as well as national cases. It should interface with civil intelligence agencies through liaison methodology thus updating threat information. The unit CI cells should be extrapolated to the creation of similar cells at all major commands which will focus on the respective area of responsibilities. These cells would produce threat and vulnerability assessments.

In addition to these functions these CI cells should be ready to be deployed to support major exercise and contingency deployments.

These CI cells will facilitate the formulation of the commander’s information requirements as the dissemination of intelligence products to the latter will heighten his perception of the situation , also these cells can communicate two ways with the collectors on the ground from parallel intelligence units thus achieving coordination between different intelligence disciplines. Investigative leads and operational opportunities result from all these efforts.

The Army Head Office (AHO) exercises technical control, review, coordination and oversight of CI Controlled activities. *a. Will execute a system of review of CI activities , ensure compliance and proper accounting.* Will have direct control over an investigation, task the CI elements , provide guidance to operational and investigative CI activities and if necessary refer the CI activity to a sub-office. But the Head office assumes full and direct control. Monitor the management of case files and other records storage and retrieval system , processing of these and transfer to the repository , maintaining the quality assurance of of investigative reports, monitor source ops and CE projects, ensure liaison activities with other agencies are properly conducted with optimum exchange of information and dissemination of information falling under their purview in a timely manner and approve or disapprove CI case summaries.

In summary the AHO

- Provides technical support to all CI assets and coordinates and deconflicts CI activities in the deployed AO
- Coordinates and supervises CI investigations and collection activities conducted by all services and components in the AOIR.
- Establishes and maintains the theater CI source database.
- Coordinates with the HOC (see HUMINT section) for CI support to detention, interrogation, refugee, and other facilities.
- Manages requirements and taskings for CI collectors in the AO in coordination with the HOC.
- Expedites preparation of .CI reports and their distribution to consumers at all levels.
- Coordinates CI activities with senior CI officers from all CI organizations on the battlefield.
- Performs liaison with national level CI organizations.

The Sub offices will coordinate technical direction and tasking from the head office , monitor all CI activities within its area of operation and provide feedback to the head office , conduct CI investigations tasked to it by the head office , and also those that it assumes worth taking up , excepting those investigations directly controlled by the head office , ensure proper dissemination to end users as well as the head office and ensure the accuracy , compliance with CI policy of all CI reporting. Briefing commanders and intelligence officials.Liasing with external agencies and disseminating information to them that falls under their purview.

We need to have a force protection intelligence doctrine,strengthen it,define the role of MI in force protection efforts and priotize collection and analysis of intelligence on force protection threats.We need a robust HUMINT capability supported by CI—the optimum integration of both is the need of the hour.We have the LU , CI and IFSU but still we lack a viable HUMINT mission.Whatever HUMINT we have is afforded by these units directly or indirectly and we must use this to the fullest potential to counter force protection threats.To improve the HUMINT capabilities MI should assign additional resources.Duplication resulting from the efforts of the MI constituents need to be removed and the respective roles clarified.Duplication creates confusion and wastage of resources.We must have a comprehensive CI doctrine.The CI units should be staffed with more personnel , both in major cities/foreign areas and in collection activities.Analysis of force protection intelligence should be properly delegated to CI cells and to this end CI Analytical cells should be dispersed at Army Headquarters and major commands

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 pseudonyms 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. It's 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 an 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.

Purposes

In counterinsurgency operations, collocating patrol bases in population centers enables combined forces—

• To deny the insurgent access to the local population.

• To influence and assist the local government.

• To provide security.

Methods of Establishment

The same priorities of work described for combat outposts apply also to patrol bases:

• Move in with the indigenous population. The advantages are that Soldiers will have more direct contact with the local administration, the locals will identify the forces with the government.

The disadvantages insurgent sympathizers from among the masses may inform insurgents about patrol movements with relative ease, attacks on the base will have collateral damage effects, and houses cannot be really hardened against attacks..

• Build a new patrol base. Although more isolated from the population, new patrol bases are usually on chosen ground and, therefore, easier to defend. Additionally, they are far more resource and personnel intensive during construction. It is generally advisable to set aside detailed planning time before sending a combined force to occupy the terrain.

PLANNING CONSIDERATIONS FOR A BASE DEFENSE

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.

RSTA AND ISR OPERATIONS

Intelligence drives operations and vice versa. In effect the enemy situation drives operations. For the enemy situation to drive operations we must have perfect intelligence about the enemy. To this end Reconnaissance , Surveillance and Target Acquisition should work hand in hand with ISR SO AS TO ACHIEVE PERFECT SYNCHRONIZATION in the deployment and operation of sensors, assets and processing, exploitation and dissemination of intelligence.RSTA/ISR should focus on the priority intelligence requirements.Recconnaisance and Surveillance confirm or deny threat actrivities,plans,courses of action which were gauged by the Commander and his staff during planning , war gaming and sessions with the collection manager and counterintelligence specialists.By focusing RSTA/ISR on the commanders needs, his critical and priority intelligence requirements we can deploy and use RSTA/ISR sensors and assets in the most optimum fashion , totally integrated and synchronized resulting in timely and accurate information, combat information and intelligence to be disseminated to the targeting platforms.

Every operation is initiated as per plan and this planning has certain decision points.RSTA/ISR should take these critical decision points in perspective , primary perspective and focus all collection platforms and assets on these points and see to it that al information linked to these decision points are gathered , nothing left out and disseminated in time to the commander. Again for this synchronization is essential. Targeting requires proper detection of the target and evaluation of its importance. Further there should be sufficient reason to nominate the target to the attack platforms. To this end synchronized RSTA/ISR operations collect all possible information about the target and pass it on for evaluation and thereafter if the target satisfies the criteria for nomination the intelligence on the target is passed on to the targeting platform. After an attack on the target, kinetic/nonkinetic attack or exploitation operations, RSTA/ISR is required to assess the effectiveness of the attack.

DETECT

HPTs need to be detected and located accurately in order to engage them and here is where all assets available to the Commander must be used to maximum efficiency.HPTs are critical nodes in the insurgent network.Engaging and destroying them successfully can render the mission of the insurgent group unsuccessful.

The priority intelligence requirements associated with the HPT should be carefully defined and resources allocated accordingly to get intelligence on the target. As time goes on and collection assets bring in information in line with the priority intelligence requirements the situation development for the commanders needs is more accurate and continuously updated. Detect the HPT involves tracking him as movement is a factor. Detecting involves assets like HUMINT source,

an anonymous tip, UAS, a combat patrol, SIGINT, DOMEX, rotary wing aircraft, military working dog teams. The best means of detecting a target during an insurgency is HUMINT, such, the detect activity requires a detailed understanding of social networks, insurgent networks, insurgent actions, and the community's attitude toward the counterinsurgent forces. For a target that must be engaged by nonlethal means, the detect function may require patrols to conduct reconnaissance of a leader's home to determine if they are there, an assessment of a potential project, or attendance at a greeting to meet with a leader.

COIN

Intelligence Support to Targeting

Refer to chart for details:

ATTACK THE NETWORK CONCEPT

http://securityantiterrorismtraining.org/FM.php

COIN Specific Intelligence Preparation of the Battle space (IPB) – the systematic, continuous process of analyzing the threat and environment in a specific area with the NETWORK in perspective.

The commander uses IPB to understand the battle space and the options it presents to friendly and threat forces.
By applying the IPB process, the commander gains the information necessary to selectively apply and maximize his combat power at critical points in time and space on the battle space.

Irregular Warfare IPB
The principal difference between IPB for a conventional warfare environment and that of irregular warfare is the focus on people and the accompanying high demand for detailed information (e.g. – census data and demographic analysis) required to support the commander's decision-making process.

Force protection in a COIN environment is dependent on several factors. These factors can be studied and detailed by compiling all data, demographic, human terrain, enemy, environment and census. The intelligence preparation of the COIN battlefield is very different than that of conventional battlefield. Here we are concerned with specific physical data so as to be aware of ambush points, egress and ingress routes,corridors,avenues of approach for the enemy, areas or profiles which can serve as cover for our troops if the enemy launches a surprise attack, areas which can provide a good cover for the enemy and which can serve as good concentration zones for their personnel etc.Hence intelligence preparation of the battlefield is of prime importance to avoid mishaps like Dantewada and the Kashmir cases. In case of jungle warfare this is more important and severe constraints are imposed due to very thick foliage, canopy, water areas, darkness etc.HUMINT is something which might be the only intelligence discipline which can work, other assets being degraded in performance/capability due to the jungle environment.CI support is to HUMINT of prime importance, particularly in inhabited areas belonging to the local community

as the insurgents HUMINT source is the same local population. This will be detailed later as to how to employ CI techniques in a COIN environment.

While preparing the intelligence assessment of the battlefield in a COIN environment we need to consider the geospatial aspects in its entirety. To achieve this we must put on paper a mapping of all explosive hazards attributes and movement patterns of the people and insurgents. Detailed tracking information should be mapped out on map and imagery templates. This tracking g information can be the event and movement patterns of the community people and insurgents prior to, during and after an explosive hazard detonation and the emplacement of explosive hazards, types, composition, method of emplacement etc.Thereafter pattern analysis coupled with terrain analysis can be executed on these information.
To enable mapping consider the following:

1. All EH detonations, arrest of people with EH devices over time need to be tracked and displayed graphically on a map template.

2. The technology used ,whether the EH was buried or thrown at the security forces , whether it is of blast fragmentation type or shaped etc need to be documented. This will yield the operational characteristics of the enemy. Again every EH needs to be tracked...keeping a time frame in perspective.

3. Every IED explosion or seizure translates to information about the bomb maker –his signature. Examine the IED to ascertain the nature of ingredients, technology used, tactics etc.Again map out this signature profile for every IED.

4. Map the IED events density over the area. Locations, dates and frequency need to be used as reference points.

5. Considering only the type of EH used if mapping is done then we can get a good idea of sources of particular types of IED or any other interpretation.

6. Keep in mind that one should track all EH events with respect to adjoining structural, organizational, religious entities. For example there can be a local village near frequent IED explosions that is hostile to our security forces. Or say a religious unit is nearby which is pro-insurgent. These entities can be processed for more intelligence.

7. Map out those areas of the physical terrain that can act as good ingress and egress points/routes/corridors to potential sites for EH emplacement.

8. Recorded information about the flow of enemy personnel, weapons, etc need to be considered in its entirety.

9. From all these EH events based mapping identify/locate areas which may be used for deployment of Ordnance/EOD /Engineers personnel and equipment preferably under cover to assist in rapid response to IED blasts or attempts for emplacement.

10. Map out all the routes usually taken by the security forces , especially in friendly areas and study the corresponding terrain in detail so as to ascertain any area/s /points worthy of IED emplacement /vulnerable to IED and post IED attacks..Identify those movement patterns of the security forces which are very frequent and hence liable for IED'ing.

11. Identify those areas where emplacement of an IED can potentially cause harm to security forces but not to the local community shelters. Of particular note are those communities who are pro-insurgency.

12. Of all the possible emplacement areas on the map identify those areas that can serve both as emplacement and also offer terrain advantages for immediate secondary gunfire attack by hidden enemy personnel.

13. Map out those areas of the physical terrain which can multiply the IED explosion severity by virtue of natural structures and profiles.

14. Locate and map all areas that can offer good concealment for ammunition and weaponry caches and IEDs.

15. Map HUMINT.For example an insurgent operative was arrested in a certain area away from his place of residence, another defined area.

16. (6) From all the EH points on the map identify those that are of low damage capacity than those that inflict mass casualties. The former takes less time for emplacement and difficult to prevent compared to the latter. Color code these two type—thus a geospatial of

such ‘’White-noise’’EH devices and ‘’Mass-casualty; EH devices help the Commander to get a better understanding, his situational awareness is heightened.

COIN targeting necessitates overwhelming intelligence from **‘’bottom-up’** for successful kinetic/non-kinetic operations. **Hence ground level units need to be trained and tasked with intelligence collection.** It is near impossible to dedicate the very few specialized intelligence assets to all the operating forces in the area of operations. Here are the key challenges of bottom-up collections:

1. Determining what is important information. Leaders need to determine PIRs for each mission.

2. Determining where to start – in terms of information or geography. Based upon key terrain (human and/or geographic).

Conventional operations and COIN/Antiterrorist operations (This can be termed operations against networked criminal enterprises) are different in that the intelligence preparation of the battle space takes into consideration not only threat elements but also the human terrain—that is the local population. Unlike kinetic attack priority in conventional operations (kill/capture) in COIN operations non-kinetic attack modes are often the desired outcome – non-kinetic attacks taking into account civilian community heads, population psychological operations, insurgent targets social network, targeting his social contacts to judge his resultant movements and tracking him to finally locate his cell members or leadership, exploitation of targets other community traits—in effect besides personality targeting we are also concerned with the fact (non-kinetic fires) that units must project the second and third order of effects after they mount any operation. Operations on a population, with which the targeted individual interacts, may have second and third order effects on that targeted individual (e.g. – he may increase communications or flee the area—in the former case SIGINT intercepts can yield a lot of information about his immediate network , if his communications are verbal and physical meetups surveillance will be the preferred tool whereas in the latter case if he flees the area he can be tracked to know his sanctuary—he is bound to contact his team members , move in their hideouts.).All in all kinetic attack fires can yield much more intelligence than just by acquiring battle order intelligence. Only resorting to kinetic fires of kill/capture can never solve an insurgency problem., As the soldiers on the ground are those who are frequently in direct contact with community members (and hence those of them who are affiliates/sympathizers/facilitators of the insurgents) they have the best opportunity to gain intelligence information by conducting tactical questioning (patrols, checkpoints, choke points) or by casual elicitation methods in normal scenarios.

Later it will be shown that setting up a company level intelligence cell and enabling tactical teams with intelligence assets gives a major thrust in intelligence collection and also counterintelligence activities.

There needs to be a change in focus of effort between command levels.

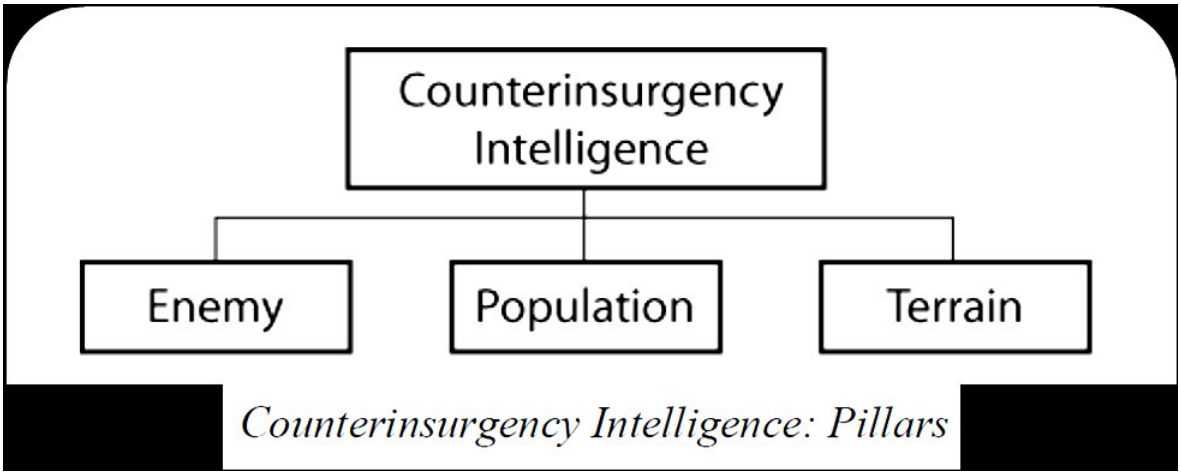
1. Stress should be given to the fact that tactical company and platoon level units conduct operations with a high degree of success and hence higher levels of command must push intelligence staff and information down to lowest points of collection (initial points) , that is the company/battalion levels.

2. At the same time low density high demand ISR assets need to be stretched and spread across the area of operations to gain a better situational understanding.

With these two initiatives the Command Headquarters will not lose control over its intelligence assets and will neither lose the privilege of gaining situational understanding exclusively. On the contrary it will be able to gain more accurate intelligence inputs. Till so far the intelligence needs of individual ground units or any feedback from them was generally ignored what with the Battalion intelligence officer forwarding the intelligence summary report to higher headquarters with the overall intelligence picture of the area of operations falling under the Battalions jurisdiction.

REQUIREMENT FOR INTELLIGENCE COLLECTION AT UNIT/PLATOON LEVEL:

It is near impossible to allocate specialized intelligence assets to every operating force in the Area of Ops, as such assets are few in number and the fact that majority of the information required for targeting flows ‘’bottom-up’ (that is the lowest level troops) necessitates the creation of intelligence collection units at troop level either organic to the tactical combat ground unit or as a modular unit capable of plugging into any company or unit as per requirements. This fact should be taken seriously into Staff consideration for targeting, particularly in asymmetric type warfare where the network must be targeted and where delivery of fire-power is dependent on very specific intelligence.



Counterinsurgency Intelligence: Pillars

Building the Intelligence Picture

a. Insurgency has its HUMINT base among the ‘’people’’, hence it becomes very important to know the human terrain, that is physical description, name, location, relationships, biometrics, job, etc. All these information are more rapidly accessible by the lower levels units like the company and platoons/sections. Lieutenants and NCOs can utilize their leadership appropriately in this regard by detailing their men to extract information about the human terrain. The lowest level that is the sepoys/soldiers can be trained to use tactical questioning to get this information. The CLIC is ideally suited for this purpose as a unit. We must incorporate female soldiers took to handle the feminine component of the local population—they are averse to be questioned by male soldiers, and the traditional conservative approach of rural/semi urban families prevents access to womenfolk by male soldiers. We must remember we are operating in an irregular environment, not in a conventional warfare setup; hence we require very specific information. After collection by the lower level echelons the information is evaluated and transformed into intelligence products and then exploited via the targeting process.

What exactly is targeting? Targeting is just not kill/capture—the kinetic component of warfare. We have both kinetic and non-kinetic fires, selected as the case may be. Particularly in an asymmetric environment like COIN operations, we are more concerned with the population. We need to create conditions among the population which will act as enablers for the COIN operation. Hence targeting is not just concerned with degrading the enemy’s capabilities. In the past we have had our special forces go out on missions with a specific objective in mind, as against our conventional warfare setup where targeting is distributed, not personality based and aimed at the enemy’s command and control nodes, logistics and weaponry systems. But here in case of COIN target engagement is like those of our special forces in the past where conventional forces act like

special forces with ‘’personalities’’ in the objective window. The targets are ‘’individuals’’ and ‘’populations’’, where we are concerned with ‘’second-order’’ and ‘’third-order’’ effects on the ‘’population’’ of our actions against the targeted’’ individual’’.(For example we can conduct certain operations among the community population which will either make the targeted individual flee the area or prompt him to contact his connections amongst the population or he may resort to communicating with his men outside the community periphery—in all these cases we can have a surveillance and signals \intercept setup on him and track these movements/communication intercepts).Hence commanders must understand this very important concept—We must not limit COIN operations only to kinetic targeting, we must consider the second and third order effects of our delivering effects on an individual; we must take a holistic view—a system comprising our forces and activities, the insurgent/s and the population. Even if we successfully identify and track a individual and have the capability to kill/capture him at any time according to our wish ,sometimes it’s better not to and let him loose and keeping him under surveillance , we further carry out non-kinetic targeting operations (psychological for example on the community leaders who we have reason to believe sympathize with the insurgents) on the community population to ascertain the second and third order effects to know more about the targeted individual and his network.

Kinetic and non-kinetic Personality targeting: Intensive intelligence activity is required in a COIN environment to single out ‘’personalities’ either for kinetic or non-kinetic targeting. Personality targeting is not always killing or capturing the insurgent. It can be the manipulation of the target, exploiting him, reaching out to him (also community leaders and individuals of influence, power) through meetings, negotiations—in short exerting influence on him so as to determine members of the larger network, plans, foreign influence and anything of counterintelligence interest. Compare this with warrant based targeting where the prosecution of the insurgent by the Law instills a confidence in the population and lends a semblance of credibility to the operation in that ‘’look these guys are following the Law instead of killing them’’.The idea of kill is never the solution, an insurgency can never be put to an end by killing alone. The forces need to positively influence the population and also carry out psychological ops and exploit the enemy to its advantage by resorting to non-kinetic personality targeting. True we also have to resort to kinetic targeting, either to remove the target completely from the insurgent network thus putting an end to his influence on the network or to remove him temporarily so as to reach certain counterintelligence objectives, say leading to apprehension among the members, forcing them to make contacts or any other action that can, if placed under surveillance, lead to important information about the enemy. Whether it is kinetic personality targeting or non-kinetic, we need to determine the best course of engagement after collecting sufficient intelligence on the targets

influence in the insurgent group and how much that influence can be removed by which method of engagement and our influence imposed both on the target and the group.

Targeting the entire network and targeting the individual have each a difficulty rating. In the case of the former the task is of much greater magnitude than that of the latter where the counterintelligence operative is facing the least opposition force—the single individual. Collecting information on the network as a whole is difficult but targeting an individual after accessing him in whatever way possible results in much detailed information after execution of a series of influence-based personality attacks.

It is much easier to categorize targets, as then particular targeting effort can be applied to each category leading to manageable chunks of information—a quantum approach to intelligence collection. Targets can be classified by function in the group, to what degree that function influences group decisions and activities and how much is the accessibility of the individual. Another category from the local population perspective can be those insurgent individuals who are in close liaison with community members. Categorizing and grouping such individuals is a must so that operations can be conducted on each separately without any confliction.
It is very important to consciously use targeting techniques rather than as a consequence for which the Commander was not prepared for. This can have an adverse reaction on the population. Hence it's very very important to execute continuous intelligence collection and management with clearly defined intelligence priorities. It should be understood that often choosing to target an entity may jeopardize the targeting objective on another. COIN targeting operations are never linear like in conventional warfare.

Right from the Command headquarters down to platoon/section level as well as adjacent companies/Bn – all of these need to be part and parcel of the target management process. It can so happen a target in one Area of operations being tended to by a Bn also influences the insurgent operations in another Area of operations. Or there could be an area far from the geographical boundary of the disturbed area but under the Command where insurgency is at its nascent stage (or insurgents have flee'd from this disturbed area and are preparing to secure that area for their operations and projecting the latter into the disturbed area with that area as base) and the insurgent HVT and HPT directly or indirectly affect the insurgents decision making processes in that new area.
To create such a targeting management system we must identify all players from a holistic point of view , not only the enemy but its sympathizers in the local population , its direct supporters , the material flow circuit in terms of money , weapons , fooding and the sources of availability of these

, and all hostile and benign aspects of the enemy. Thus we are not preparing to attack only the enemy but the ENTIRE NETWORK.

The Command headquarters should lay down SOP for identifying and nomenclature of Targets so that uniformity is maintained at every level, vertical and horizontal throughout the Command. This will also facilitate the systematic management of the Target folders database. It could be that the standard method of nomenclature may not apply to all targets as some may overlap in terms of capability, position, multiple lines of operation or categories. Certain disciplines such as SIGINT and IMINT will use their own methods of nomenclature and categorizing, different from HUMINT methods. Here it should be seen that although we cannot change their methods of nomenclature, the manner they feed into the ‘’targeting process’’ should translate to the standard laid down by the Command headquarters. Still the standard should attempt to introduce uniformity as far as practicable across all echelons of Command.

With the company level intelligence cells, the Bn intelligence platoons providing intelligence up the chain and the ‘’top-down’’ standard mentioned above will foster cross-leveling and coordination of targeting information provided by those units/cells.

Categories:

Kill/Capture: The most common category. **The equation that a kill is a kill is not valid in COIN.** Killing one insurgent ***can create 3*** out of feelings of vengeance. It’s very important to have a holistic view of the entire COIN campaign including the local population and target centers of influence (for and against the campaign) with appropriate techniques, **finally isolating** the enemy from its support base and **then going in for the kill.**

Detaining for prosecution: Strategic communications, key leader engagement, and civil affairs fall in this category. Here we need even more intelligence so as to obtain a conviction in the Court of law apart from identifying and apprehending the convict. Getting him convicted rather than killing him won’t raise the issue of vengeance that much and the local population too will appreciate this element of legality in the operations as everyone is opposed to killing. Sometimes with the process of engaging targets and external influences, it might be justified to convert a target with the kill/capture tag to that of warrant based targeting.

Influence Targeting: Key community leaders, those elements of the population who are pro-insurgency and lend direct/indirect t support, enemy couriers/prisoners who may be “turned” by CI agents to get inside information, those who are anti-insurgency and those that facilitate the enemy’s TTPs but project a clean image.

Counterintelligence Planning

Planning of tactical operations includes CI planning. This is an extremely important component of the overall planning. As CI/HUMINT operations require much more time than other intelligence disciplines these are looked into at the very beginning of tactical operations planning by the Commander.,It is the CI staff officer who assists in the planning. He may further be joined by the Human exploitation team officer in charge and the CI second in command.

Requirement:CI planning is required as it aids the Commander in situation development.The commander can asses security vulnerabilities, get an estimate of the threat intelligence and force protection factors.It also helps in the overall formulation of intelligence and force protection operations.During planning overall intelligence effort certain intelligence disciplines like HUMINT have close ties with CI—hence the need for clear CI planning.CI activities and HUMINT operations need to be integrated and deconflicted as both have similar methodology , CI focusing on threat intelligence and countering it while HUMINT focusing on collecting information about the enemy.Effective human exploitation (such as sources,refugees,EPW etc) such as using interrogation/translation to extract information of intelligence value from EPWs. During the planning phase of tactical operations CI information is made available to the Commander and countermeasures suggested. The commanders benefit from CI information given at this phase because it helps to formulate tactical plans and because CI/HUMINT operations, by their very nature, generally require

more time than other intelligence disciplines to yield substantive results.CI looks outside-in and hence the CI staff officer participating in the planning phase advises the Commander on the vulnerabilities which enemy intelligence may target.

The commander formulates an all-source intelligence collection plan to which the CI staff officer contributes by:

A)Assisting in giving direction to the planning by focusing on the enemy's intelligence,subversion,terrorism and sabotage capabilities..

b)Making it sure by coordinating with the intelligence operations officer and collection manager who are also present in the planning that the collection requirements levied on the CI/HUMINT operatives are in tune with the Commanders intelligence requirements and that the CI elements have the capability to pursue the activities thus helping the overall collection plan by inserting such realistic factors,

Planning the Activity. The CI Staff officer along with the help of the CI/HUMINT Company commander directs the collection effort—collection of intelligence pertaining to the enemy's intelligence,terrorist,subversive,and sabotage capabilities,oversees the production of the said intelligence,ensures the timely dissemination to higher-ups and the units on the ground and finally recommends and monitors CI measures throughout the Command.Throughout he is assisted by the Officer in charge of the Collection Deptt and the Operations Staff.

CI Planning Considerations. Key considerations in planning CI operations include:

Determine clearly the Area of Ops and the Area of Interest.The concept of operations,the command/support relationships between HUMINT,CI and Reconnaissance units.,What are the intelligence requirements which the supporting CI units have been tasked with?What are the priority intelligence requirements,whether it's the enemy ground/air ops,target battle damage assessment or future intentions of the enemy?

Enemy Considerations. Intelligence operations are designed to know as much as possible about the enemy.Key points are:

What are the threat forces characteristics?Are they guerilla type or do they belong to terrorist,insurgent organizations?Is there any sabotage group involved?Are there any enemy HUMINT/CI personnel?Are we handling an enemy with the forces structured on conventional lines or is it they are loose asymmetric cells?What are their centers of gravity and vulnerable nodes?Their sizes,composition,TTPs?

Who are their Commanders and key leaders?Their C2 nodes and associated vulnerabilities?What are the TTPs of its C2 and CIS systems?What is the CI structure and what are their CI measures to prevent CI exploitation?

Who are the known enemy personnel engaged in intelligence,terrorism,sabotage,insurgency , CI or security activities?Who supports them /sympathizes with them from among the political/administration or population domains?

What are the key physical facilities,including installations used by the enemy? What are the key communications, media, chemical,

biological, utilities, and political installations and facilities?

Which political parties,student groups,political/national figures and student leaders support the cause of the enemy and are hostile to our country?

CI planning and execution is conducted in concert with the six phases of the standard intelligence cycle. The first phase is planning and direction. It consists of those activities that identify pertinent intelligence requirements (IR) and provide the means for satisfying those requirements (see figure 6-4).2 Intelligence planning and direction is a continuous function and a command responsibility. The commander directs the intelligence effort; the intelligence officer manages this effort for the commander based on the intent, designation of priority intelligence requirements (PIR),and specific guidance provided during the planning process.

Planning and Direction Functions

- Requirements development
- Requirements management
- Collection management
- Production management

CI Planning and the Intelligence Cycle

Operations drives intelligence.Intelligence drives operations.This dynamic is the essence of mission-based intelligence support and is carried out by flexible and not rigid application of the intelligence cycle.The intelligence cycle is not an end in itself.Every intelligence requirement undergoes processing separately.Planning is continuous.As the operations proceed further intelligence requirements surface and older ones are modified.Counterintelligence planning is composed of two iterations of the intelligence cycle…Decision planning and execution planning.In the first phase the battlespace and threat is determined by processing basic intelligence and counterintelligence procedures (collection,collation,analysis of information of intelligence and counterintelligence value) resulting in the production of intelligence and CI estimates and the intelligence preparation of the battlefield.Using these end products the Commander now goes forth to develop and select the various COAs.Now the second iteration , viz execution planning takes place.For every COA selected the resulting scenario is studied and the concept of operations determined.Keeping the mission in perspective,and based on the concept of operations,refinement of the intelligence and counterintelligence variables occur together with a review of the IPB,implementation of the final intelligence and counterintelligence collection,production and dissemination plan,the end products of which are mission-specific intelligence products and CI measures for the Commander to integrate with the concept of operations and conduct mission execution.As execution proceeds fresh intelligence requirements surface and each requirement is given unique attention,satisfied so as to ensure smooth mission execution.

Information Operations are the key to win a war by establishing information domination.To this end intelligence assumes prime importance and like it counterintelligence is a force enabler by responding very aggressively and effectively against enemy ISR operations.CI is particularly suited for enemy asymmetrical threat.Thus counterintelligence lends credible support to information operations. The enemy ISR capability ranges from traditional HUMINT operations to highly sophisticated computer penetration operations. CI operations provide multi-discipline CI analytical support to planning, security, and targeting. CI agents conduct threat assessments,vulnerability analysis,investigate intelligence security violations,detect and counter threat ISR operations/capabilities and recommend possible countermeasures to the commander—all in all intelligence and counterintelligence shape the battlespace in the most optimum manner to accomplish the force mission.

TECHNIQUES

CI techniques are vulnerability assessments , intelligence simulation of adversary activities also called red teaming and covering agent support.

CI techniques are means used to accomplish the mission efficiently and effectively. Selection of techniques occurs at the lowest level possible by the on-scene CI element to meet the needs of the supported military commander within the constraints of the operation and applicable regulations. Techniques include vulnerability assessments, hostile intelligence simulation (Red Team), and covering agent support.

VULNERABILITY ASSESSMENTS: Every command has (and should have) an internal force protection program.Such programs are the target of enemy intelligence services for exploitation. The command , because of vulnerabilities , becomes susceptible to enemy intelligence collection.This is an essential component of military security.Even operations should be aware of any vulnerabilities which are liable to be exploited by the enemy.Vulnerability assessments provide the commander an effective way to evaluate internal security/force programs of a Command , headquarter , installation or operation. The objective is to pinpoint these vulnerabilities , remove them thus enhancing the overall security of the command or headquarter/installation.

All adversary multidisciplinary threat intelligence activities should be monitored , evaluated and analyzed. Included are adversary collection capabilities and platforms and all intent discerned by the CI staff.

Bing totally aware of all our activities , operations , patterns of these, our physical and electronic signatures

Monitoring and collection of all CE transmissions , which will be of help in creating a good foundation upon which the CI agent bases his decisions to recommend suitable countermeasures.

Based upon all the above collected information about the adversary and our own command/installations and operations , analysis is conducted and countermeasures suggested.These countermeasures are further studied for effectiveness index both prior to and after implementation.

HOSTILE INTELLIGENCE SIMULATION (RED TEAM): A command may be penetrated by the threat intelligence service. The same goes for any installation , operation or even a security/force protection program designed to offset such penetrations. Whatever be the case if the commander can gauge enemy intentions the better will be able to decide on his course of action. To this end he employs counterintelligence personnel to simulate an enemy penetration of a specified target , say an installation or a program. The enemy's intelligence capability is not limited to a few. There is an array of disciplines which the enemy can resort to. The counterintelligence agent , while conducting red teaming , will use this multidisciplinary counterintelligence approach in that he will employ selectively (for each target which the enemy will try to penetrate or exploit) those MDCI resources which are more appropriate for the enemy corresponding to that particular target , say perhaps overhead photographic reconnaissance or communication and signals intelligence. During the vulnerability assessments the CI agents uses similar multidisciplinary intelligence techniques to know about the enemy.

Red team operations should be as realistic as possible , should involve only very experienced CI personnel , and total coordination is needed with other technical staff , intelligence personnel , the unit commander and all who are connected with the internal force protection or security program.

Commanders must ensure compliance with laws, policy, and regulations when employing COMSEC monitoring, electronic surveillance, or other technical CI collection activities as part of Red Team simulation operations.

Red team operations involve highly technical resources such as COMSEC monitoring , electronic surveillance etc and going by the complexity and these high resource requirements red team operations should be applied to those assets , activities which are highly sensitive.

Red Team operations lead to revelation about weaknesses and vulnerabilities which are documented first in a operation plan , then studied/evaluated and then recommendations are made as to how to reduce these vulnerabilities and employ proper countermeasures to these vulnerabilities , how the security posture of the command can be enhanced, what security education need to be given or what content need to be added to current security

education/.programs of the commanders and their security staff to enhance the effectiveness of their security policies and practices.

COVERING AGENT SUPPORT: When the CI dep't is requisitioned to extend its services to a particular command or unit it may detail an agent as liaison officer and also as a supporting special agent to the command/unit. This agent will conduct all routine liaison and advice/assistance with the supported command/unit. Areas of interest like operations , security , vulnerabilities , personnel will be studied in detail by the agent till he becomes thoroughly familiar with them and in turn he acts as a point of contact for the supported element to report any matter warranting CI advice/assistance or in other words of potential CI interest.

Tactical CI Tasks

Source operations. The top priority for any force is the protection of its personnel,installations.Source operations are conducted for force protection.(elaborate).

Screening and interrogation of persons possessing information of CI value.Instead of always conducting rear operations(interrogation centers are usually located at the rear) which entails poor performance as on several occasions intelligence is time sensitive and perishable,CI/HUMINT teams are deployed at the front wherein if HUMINT agents find someone with information of CI value,he can be rapidly interrogated there and then.The HUMINT and CI components can both conduct screening to determine appropriate individuals. Thus mobile interrogation teams make matters much manageable.

- Interrogation of EPWs.Debriefing of recce patrols turned EPWs and detainees.
- CI investigations.CI Review.
- Document exploitation DOCEX.
- Conduct evaluation and analysis of seized equipment/hardware.
- Conduct CI surveys and act in advisory capacity to the Commander on vulnerability issues by resorting to red teaming
- Conduct TSCM operations
- Analyze CI and terrorism threats and assist in the preparation of plans, estimates and orders
- Take control of the interrogation and documents/material exploitation centre and supervise the proceedings and intelligence activities
- Assist in the identification and recovery of missing and captured personnel

Authorities set up—Management committee for managing CI and HUMINT.

- Director –CI and HUMINT
- CI cell with a CI coordinator in charge
- HUMINT Ops cell

Tasks of all three:

Coordinating, managing, deconflicting technical control and proper dissemination/reporting of:

- Interrogation and debriefing activities,
- Mobile Interrogation activities,
- HUMINT source operations,
- CI operations pertaining to Force Protection,
- CI investigations,
- Other overt HUMINT operations,
- All covert and/or special compartmented HUMINT operations.

Three types of measures employed in CI operations are **denial, detection, and deception** of threat intelligence collection efforts.

Denying the enemy and its intelligence apparatus any information about our installations,personnel,information and operations is vital and cannot be overemphasized. Similarly we must resort to deceptive measures to present before the enemy intelligence a fabricated version of our actual intentions and operations so that the enemy is misled and is forced to utilize and deploy its resources in the most disadvantageous manner and be susceptible and vulnerable to our targeting, whether lethal and kinetic or psychological. Detection is all important and facilitates the proper usage of denial and deception operations.

We must detect the enemy's intelligence efforts at the earliest. Here is where I&W plays a very important part. In addition offensive counterintelligence such as infiltration and penetration coupled with enemy agent exploitation can give us an inside view of the enemy's organization, its operations, its key intelligence personnel, our turned-personnel and its intentions. Detection examples include checkpoints and roadblocks thus creating choke points to to enable screening and to control the vehicles and personnel in the area of operations. Such checkpoints enable our agents to detect enemy agents ,false identification papers and caches of arms, ammunition and equipment.

Denial measures include document security, physical security of our installations, signals communication security,counter-reconnaisance and censorship.

Deception consists of feints, ruses and fabricated information leaked to the enemy—all of these can have several objectives, like depleting the enemy's resources wastefully thus reducing his combat effectiveness-example being forcing him to direct its firepower in a massive operation on fake weaponry systems,hangars,ammo dumps ,defense facilities etc.The intention is to mislead the enemy about the status of our combat strength,logistics,dispositions,firepower,and other activities. Deception operations are normally planned, approved and directed by higher HQ's.

CI measures can be either offensive or defensive in nature.

Offensive CI measures are aggressive in nature. They are intended to prevent the enemy to gain information by employing sabotage or subversive activities. On the other hand Defensive CI operations are directed at conducting security reviews, vulnerability analyses, secrecy discipline, security of documents and materials which are of sensitive nature, signals security and overall security of the installation.CI Defensive measures constitute a portion of the units SOP.

The primary mission of CI focuses on force protection.OPSEC,Deception and rear area operations like interrogation/debriefing at interrogation centers and securing rear area facilities and base camps/headquarters are used to this effect.CI resorts to aggressive measures to degrade the enemy's multidisciplinary threat intelligence and targeting capabilities. Here in intelligence parlance, targeting does not only mean physical or behavioral degradation but also intelligence collection products.CI is multidisciplinary , involving all three—C-HUMINT,C-IMINT and C-SIGINT.

Force protection is a command responsibility to protect personnel, equipment, and facilities. To carry out his force protection responsibilities, a commander requires support from several sources, one of which is the intelligence community. CI support to force protection must be tailored to the sensitivity of the supported organization and its vulnerability to foreign intelligence service (FIS) and hostile attack. CI support can be tailored from a combination of activities to include:

- Mobilization security, including ports and major records repositories.
- Combating terrorism.
- Rear operations.
- Civil-military affairs.
- Psychological operations (PSYOP).
- Battlefield deception.

- OPSEC.
- Friendly Communications-Electronics (C-E) (C-SIGINT).
- CI force protection source operations (CFSO).

> Army CI is not limited to the activities of a small force of CI agents and technicians; rather, it is the responsibility of all Army personnel to follow common sense security measures to minimize any foreign intelligence threat.

Although a major part of the CI mission is to counter or neutralize FIS efforts, this does not mean that only

CI personnel take part in these actions. They may require:

- Other intelligence specialists such as interrogators.
- Military police (MP).
- Civilian counterparts and authorities.
- Combat forces.
- Civil-military affairs and PSYOP.

CI is that phase of intelligence activity aimed at destroying the effectiveness of enemy foreign intelligence

activities, and at protecting information against espionage, personnel against subversion, and installations or materiel against sabotage.

CI MISSION

CI MISSION: The mission of the Divn CI is to counter threat ISR efforts , act as a support to other intelligence disciplines especially HUMINT,support targeting,FP,and advice the Commander and recommend security measures.

CI personnel are engaged in three basic operations:

- CI Investigations
- CI Assessments
- C-HUMINT Ops.

COUNTER-HUMINT OPS-TACTICAL HUMINT TEAM.

*Counter-HUMINT OPS has as its Primary mission to report on enemy ISR activities,the information being collected by exploitation of human sources and documents.These reportings are done by the HUMINT portion of the tactical HUMINT team.As for its Secondary mission,the assessment and neutralization of threat ISR activity is conducted by the CI element of the tactical-HUMINT team.*The tactical-HUMINT team also called the HUMINT Platoon consists of a headquarters element, a HUMINT Control team, three HUMINT Teams and one CI Team(normally 4 soldiers further subdivided into two-soldier groups)

The CI team performs three basic operations: CI investigations, CI assessments and Counter-HUMINT operations.

CI OPERATIONS

SPECIAL OPERATIONS:

Here the enemy intelligence service is engaged directly using human source or technical means.Operations can be classified as offensive operations and defensive source programs.The former actively , continuously and offensively engages the enemy intelligence service whereas the latter concerns itself with protecting designated activities/operations from the enemy HUMINT threat which has been confirmed to exist and is active.This C-HUMINT also engages the enemy intelligence service but the prerogative is protection.In the case of offensive operations , there may be penetration , infiltration , offensive exploitation , neutralization of the enemy intelligence service (and / or its agents) on a war footing.

GENERAL OPERATIONS:

CI general operations are essentially defensive in nature and are aimed at supporting the force protection programs and formal security programs of Army commanders at all levels. Included in general operations are

- Advice and assistance programs.
- Technical support activities.
- Support to intelligence disciplines.
- Support to treaty verification.
- Support to domestic civil disturbances.
- Support to HUMINT.
- TSCM Ops.

- Planning and recommending security measures , inspecting facilities , installation components , and all other assets that warrant security review and resolving security issues.
- CI surveys and technical inspections.
- Advice and Assistance Programs. Installations , units and Commands have a security plan in place and SOPs.But these tend to be routine , generally following age old military traditions or as laid down in standard doctrines.The adversary of today is much more smarter than what he was just 10 years back.He is more unpredictable , more agile , more adaptable thus changing his tactics/strategy with our implemented securiuty plans and now he has a very efficient intelligence capability which helps him to know what is being don't to secure our forces , equipment, information and operations.CI teams undertake the responsibility to gauge enemy behaviour in advance and accordingly set up advice and support programs to enable the Commander to implement much better security programs and educate the personnel on security issues.With these advice and assistance programs in place , enemy intelligence activities , specific vulnerabilities in the units security system which are not yet in the knowledge of the security officer are identified and corresponding countermeasures incorporated in the security programs and SOPs of the Command/unit/installation.Such threats to our securitry from the adversarys intelligence service can now be effectively neutralized and the enemy denied access to information about our forces , plans and operations.

Support to Force Protection and Information Ops Planning is the domain of CI operations.CI ops identify the vulnerabilities of the military force to enemy multidimensional ISR threats and recommend suitable countermeasures.CI ops include CI Security investigations, CI analysis and C-HUMINT operations conducted by the Tactical HUMINT team.

CI INVESTIGATIONS.

Counterespionage investigations and Personnel Security investigations are the two types of investigations conducted by CI agents.The former deals with cases subversion,espionage,treason,spying,sedition,sabotage and CI aspects of terrorism/assassination whereas the latter is conducted to determine suitability of personnel for security clearances and also to assist the commander to grant limited access authorization to foreign nationals and indigenous personnel.

CI support to vulnerability assessments.

The enemy conducts MDIC (multidiscipline intelligence collection) activities to ascertain the vulnerabilities of our installations,bases,facilities and other locations/assets including semi-permanent ones.The CI team conducts these vulnerability assessments by red-teaming and other methods and recommends suitable countermeasures to the Commander.Military police,engineers deptt and other units assist in ascertaining these vulnerabilities.On-going ops are also scanned for vulnerabilities so as to maintain operational security.

COUNTER-HUMINT OPERATIONS.

Counter-HUMINT operations are operations to determine adversarial intelligence threat by identifying the enemy's HUMINT collectors and either neutralizing them or exploiting them by using deception techniques or by recommending security or targeting steps.CI operations are either Special ops or General ops , the former being aggressive in nature with direct or indirect engagement with the enemy's intelligence service using human agents or technical measures. Infiltration and penetration operations are two of the various Special ops countermeasures.

Counterintelligence Support to Technology Protection

The Army continually undergoes a technological transformation in terms of equipment , weaponry, weapons delivery platforms, land and aerial surveillance systems, communications,misile development,and a host of other active and support systems. There are R&D units, scientific establishments within Army jurisdiction where technological inventions, modifications and collaborations with third parties take place , some or several of which are of very sensitive nature and if they fall in the hands of enemy agents will cause the Army to lose its competitive edge over the enemy. Or in other words the technological advantage. Not only technology but the usage of technology needs to be protected also using appropriate counterintelligence measures.

Counterintelligence will:

1. Determine the threat and level of risk imposed by the threat to the research and development units, plans and blueprints repository , acquisition programs.

2. Review access protocols and educate all personnel on risk factors , how to spot subversive elements and behavior and reporting methodologies.

3. Counter the foreign intelligence services attempts to gain access to the facility and technology by conducting CI collection , investigations , review , and other operations.

Counterintelligence Support to Infrastructure Protection

Counterintelligence support to infrastructure protection includes information and information systems and databases, power grid systems, water supply systems and any other critical infrastructure which if compromised can sharply damage force protection efforts and render survivability difficult.

Generally CI support to infrastructure was limited to information systems protection but now terrorism has taken so many forms and because of its high adaptability we must now take everything into consideration , from information systems , power grid to water supplies. Here one thing is important as to delineation of roles. If it is found that the intrusion is of standard criminal nature then the law enforcement (say the equivalent of CID in the Army) takes over the investigation but if the intrusion smacks of a enemy intelligence service flavor then of course it is the CI units domain.CI support to infrastructure is essentially a force protection function and hence should always be a priority. Heavy damages can be inflicted by remotely attacking the infrastructure , thus severely undermining our defense and attack systems.

Support to Intelligence Disciplines. IEW functions such as Early Warning , situational development of the commander are further strengthened by the application of counterintelligence to intelligence disciplines that generate these intelligence products and assessments. With a rich interaction between intelligence disciplines and CI, conflict and compromise can be avoided, information vetted , source databases deconflicted and the overall intelligence activity value enhanced further.

Support to HUMINT. Countering the foreign intelligence services HUMINT operations is the major task of any CI operative. It should be remembered that CI is a total Army mission with the involvement of all concerned personnel, intelligence operatives and commander/.staff. Alone it is not possible for the CI operative/s to conduct CI-HUMINT operations effectively. CI-HUMINT Measures:

- Determine the HMINT threat , Identify the hostile HUMINT collector.
- Effect the denial of information sought by the collector , neutralize or exploit him Neutralize or exploit the collector or deny information.
- Employ denial and deception and control measures to prevent the enemy HUMINT collector from accessing the information he seeks. The same is applied to all indicators of our operations/intent. Control our own information and indicators of operations so they are not readily accessible to foreign collectors.
- Advising the commander to strictly adhere to physical, personnel and information security protocols and stringent access systems/codes. To accomplish C-HUMINT, the CI agent, individually or as part of a CI team, conducts investigations, operations, and collection.

Other tasks include

- Creating a database of multidisciplinary threat intelligence files, maintaining them, updating them with security access protocols imposed. Handling the dissemination of information from these files as per queries which respect these access protocols. The database will contain all threat intelligence collection on organizations , infrastructure,leadership,past and recent activities, locations and individuals of particular CI interest. A separate but related database will also be maintained on sources, informers and persons who are either witting or unwitting but have the potential of furnishing intelligence of CI interest in the future.
- Conducting CI reviews and background/personality checks on those individuals, contractors and armed forces personnel who are being vetted for security clearances and also those whose loyalty is under suspicion.
- Conducting education programmes for all personnel who are directly or indirectly associated with the security of installation,plans,operations,personnel and information.Included are briefings to the concerned officers of the command and the commander and his staff on the nature and scope of the multidisciplinary threat intelligence and recommended countermeasures.

- Looking for and identifying those persons who are either terrorists,saboteurs,insurgents or are associated with these categories of the enemy.After identification is complete the CI agent forwards the information to the concerned military law enforcement authority for apprehension and prosecution.
- Conducting interrogation of EPWS and debriefing of patrols, returned POWs,aircraft pilots or any other personnel who may deliver information of interest to the CI agent.
- Must be able to deal with all situations regarding security threat with a calm composed mental frame as in combat zones many people are wrongly assessed as enemy provocaeuters on account of their presence only in the combat zone.

A mix of CI teams of technicians, agents, interrogators, and analysts considerably heightens the effectiveness of an overall CI mission. By the very nature of their mission, CI agents provide area coverage and are in a position to provide valuable assistance to supported commands in countering adversary activities in those areas.

Following are expected of CI personnel.

1. Must be able to detect and acquire detailed information about the enemy's order of battle and exploit the information as well as duly report it in time.

2. Every CI personnel detailed for the mission must invariably know about his own units opposing the enemy and vice versa.
3. EPWs are a rich source of information provided the CI interrogators know what to ask them about the current enemy order of battle. That means CI personnel should maintain and update data on enemy disposition, strength, weaknesses, composition, training, equipment, activities, history, and personalities..
4. Be prepared to work in forward areas with combat units and even HUMINT personnel in addition to the rear.
5. Develop and maintain local human source networks who have access and placement to specific, accurate and timely information about the enemy , particularly force protection information.
6. Must be able to conduct vulnerability assessments , identify critical sectors of the installation and recommend security/preventive measures to the Commander.
7. Must be able to properly brief the Commander and his staff , the MP , interrogators (in case of CI agents) on enemy multidisciplinary threat , activities and force protection issues. .
8. Conducting security programs tailored to the units requirements and mission.
9. Educating unit personnel on suspicious behaviors which could indicate subversive attempts of the enemy or malafide intentions of civilian hires/contractors.

10. Conducting security reviews

Lateral units have concurrent intelligence requirements on the adversary such as terrorists , foreign intelligence services , insurgent's etc.Remember CI personnel arrive in the area of operations first and hence can gather threat information , source leads , and all other operational factors thus creating a rich repository of information for adjacent units , including civil affairs and Military Police. Thus CI personnel conduct liaison operations with all these units. To this end all activities between CI elements and adjacent units must be closely coordinated at all levels of operation.

1. Primary function of CI elements is to detect and identify enemy multidimensional intelligence collection efforts.
2. Civil affairs personnel usually keep databases on:
3. Civilians sympathetic to the enemy or in collaboration with the enemy
4. Police records , government documents , storage media, archives which can be potential sources of information
5. Dossiers/personality files on politicians and their views/stand on the happenings in the area regarding our operations and those of the enemy
6. Information on religious leaders , panchayat leaders etc who may have a bearing on the AO developments
7. Blueprints , plans of the government
8. Those elements belonging to the political domain and civilians/other leaders who are in a sense strongly against the government in its efforts to assist the security forces—dossiers on these prepared by CA personnel can give valuable insights and leads on possible enemy infiltrators.

In brief , although the primary mission of CI personnel is to detect , identify the threat intelligence activities focusing on subversion , terrorism , espionage and sabotage , both CI and CA should work hand in hand to monitor civilian feelings and activities. Just like the center of gravity of the insurgents is located among the population so is that of the COIN forces.

Both MP and CI elements frequently develop information which may fall into the jurisdiction of the other. MP and CI agents have a mutual interest in many areas and may find themselves interfacing in a variety of circumstances It is important that the MP units not only focus on law and order within the Army areas and concerning army personnel but should also keep a tab on the local criminal activities and criminal gangs/enterprises as these activities may develop into sabotage or subversive activities affecting our forces. Hence CI and MP personnel should closely coordinate with each other and with the local police and intelligence agencies (the latter keep

records of crime and law and order situation in their jurisdictions) during MP investigations, screening and during cordon and search operations. The CI and MP units should jointly organize checkpoints, both static and mobile to apprehend infiltrators or for MP imposed control measures. Both should develop an atmosphere of information and intelligence exchange.

CI Screening.

People attempt to leave the area of operations or enter/infiltrate assuming cover stories. These cover stories , to sound convincing , are based on certain true facts regarding the intellectual , cultural and psychological peculiarities of the local community. Hence CI agents need to be well informed about these as well as the prevailing political and other areas of interest concerning the area of operations and adjoining places. To effect good interrogation they must have some knowledge about the local dialect and there should be interpreters.MP , Civil Affairs dep't and officials holding interrogation prisoners should cooperate with the CI agents by giving them information about people of CI interest.

CI/HUMINT teams conduct screening operations to make available knowledgeable individuals for CI questioning, interrogation and debriefing. As mentioned earlier in this book CI screening is of primary importance, otherwise a lot of time and effort/resources are wasted in handling a large number of unscreened individuals comprising of detaineees,EPWs,refugees, and civilian internees at checkpoints and and collection points.CI Screening operations identify enemy intelligence agents, saboteurs, and subversives; enemy intelligence collection operations and capabilities; and Category II and III threat to operations areas. These CI activities are not conducted in isolation and are coordinated with Military Police, Civil Affairs, interrogation of EPW and related HUMINT collection activities, or other ongoing operations.

Force Protection Source Operations (FSO).

Force Protection Source Operations are different from the collection operations by HUMINT agents to answer commanders primary and other intelligence requirements through tactical questioning. The objective of FPSO is not a sudden intelligence requirement or intelligence gap but is something which should be a continuous consistent Endeavour , totally defensive in nature and conducted by developing and employing human-source-networks throughout the area of operations and also beyond.Developing,exploiting and maintaining these human-source-networks is a very time sensitive process and therefore are best executed in static situations or sustainment areas.Note further in the pre-deployment phase,before the boots hit the ground,HUMINT-CI teams should be dispatched with sufficient time in hand to make a preliminary but near-thorough assessment of force protection conditions satisfying FPSO objectives and also acquire all intelligence information about the area of operations from the departing force intelligence element.

Liaison.

CI personnel coordinate with adjacent units and staffs, key Army agencies such as the Military Police and Civil Affairs and maintain liaison contact with local national counterparts to obtain operational, threat and source lead information.

SCREENING OF SOURCES TO DETERMINE USABILITY

The TACHUMINT team will place the sources under the scanner to determine their usefulness. The HUMINT collector will basically place the source within one of four categories.

Persons who have information of immediate intelligence interest.They are interrogated or debriefed as the case may be on the spot.The mobile interrogation teams come in handy at this juncture.

Persons who may be of interest to other intelligence disciplines.For example the source may have information of TECHINT value.In that case the HUMINT collector can take the services of a technical savvy operative to interrogate or debrief the source.Again HUMINT collectors are presented with the ‘’profile of interest’’ by CI agents.If the source matches these requirements the HUMINT collector first extracts all what he can relevant to his domain and then transfers the source to the CI team for questioning.All this is coordinated by the OMT.

Persons who may provide good intelligence in the future by virtue of their placement and access to the enemy intelligence services or organization.The HUMINT collector after careful assessment comes to the conclusion that this individual has the potential to be a good source.As such his name is entered in the database in the folder of potential sources.

Persons who can provide no information of any intelligence value

CI PROFILES OF INTEREST WHILE SCREENING

The HUMINT elements in the TACHUMINT team liaise with the CI elements so as to know their requirements before conducting screening.This profile of interest is of two types.Persons of the enemy's intelligence service conducting collection operations fall in the first category.Persons who can provide details (identifications,locations or activities)about the persons in the first category constitute the second profile of interest.Generally CI operatives are interested in persons who :

- Have no identification documents.
- Have excessive or modified identification documents.
- Possess unexplainable large amounts of cash or valuables.
- Are illegal border-crossers.
- Attempt to avoid checkpoints.
- Are on the CI personalities list, which includes members of an intelligence service.
- Request to see CI personnel.
- Have family in the denied area.
- Speak a different language or dialect than is spoken in the area.

Examples of the two specific interest profiles are but not limited to:

- Identified or suspected elements of the enemy's intelligence services and their supporters.We must also include elements of criminal gangs ,terrorists or drug dealers who have liaison with these enemy intelligence personnel or supporters.
- Identified or suspected espionage agents,saboteurs,subversives
- Hostile political figures
- Identified or suspected enemy collaborators/sympathizers from within the local community

- Members of the underground ant insurgent groups or other groups who are willing to provide information.
- Deserters from enemy organization
- Persons who possess knowledge about enemy intentions,strength,capabilities
- Persons who in the recent past had good influence in political or village panchayat circles in the area of operations
- Displaced persons/refugees who hold information about the enemy

RECOMMENDATIONS IN CI

Deconfliction. Deconfliction in intelligence operations is a very big problem, especially in times of war. Both active and passive HUMINT collectors should be taken into account when deconflicting HUMINT and CI operations. The following need to be taken into account:

- Registries and Rosters
- Meeting venues. Meeting times.
- Source Placement and Access Management.

Deconfliction is a very serious issue and should be addressed with the aim of managing working relationships very very effectively and very clearly outlining mutual objectives.Deconflictioin is proper source administration between active/passive HUMINT collectors and CI collectors.The same source should not land up supplying the same information to different agencies requiring that information for different purposes(with the source getting paid multiple times).This also results in underutilization of the source with the latter dividing his time between tasks of the various agencies. As the span of operations goes beyond the standard chain of command (that is, national collectors, special operations forces, sister services, and security forces),, deconfliction becomes even more difficult.

The source registries and rosters in the repositories of national level agencies , tactical organizations (Army, Navy and Air force) and others should all be pulled during say a theater-level operation and deconflicted , thus creating a theater source registry(deconflicted that is) at the tactical-collectors level and inputting deconflicted source data from national level and other civilian agencies—thus updating the tactical-source registry database.Deconfliction should start from the most internal elements and progress outwardly eventually dealing with theater levels.Information levels,tactical and strategic are the two domains requiring source deployment.Coupled with this the attributes of access and placement gives us a framework to manage wherein the right sources are selected in keeping with these three factors , source rosters are maintained meticulously and operational schedules are constantly updated.(keeping all the three factors in proper balanced perspective.).

The main point is creating deconflicted source registries right from the lowest and internal levels right upto theater levels. [Note: There is an order merit or precedence (often first come, first serve) that aids in deciding the fate of sources when there is a conflict.] Once completed, we could be certain that no source was being seen, paid, or supported by multiple organizations.

Screening Cell Operations. During conflict or ongoing operations the tendency is to screen and interrogate/debrief elements from outside the wire first.For force protection reasons and for source operations local or civilian hires should be immediately screened so as to determine their placement and access to useful information.This is often overlooked.In COIN operations locals can both be a good source of information and an indirect threat.

Screening Released Detainees. Detainees who have been released can be exploited when under detention using monetary or other inducements (after they have been subjected to CI screening so as to determine their potential in supplying future information of intelligence value)so that upon release they serve as continued intelligence sources and help to develop leads.

Interrogation Facility Operations. Manage and coordinate interrogation facility operations.

Effective Use of Mobile Interrogation Teams (MITs). At the forward areas,on or near the battlefield where enemy personnel or other human elements are taken prisoners or detained, there are chances of capturing personnel who posses little or no information of intelligence value and hence detention and interrogation centers become overcrowded with associate costs going high and administrative and intelligence assessments getting affected and delays in decision making result. Moreover these people with no or less information of intelligence or target value may have to be unnecessarily transported to interrogation centers in the rear area if not screened and interrogated properly which exactly why we require mobile interrogation teams MITs composed of CI personnel.These agents , when handed over captured or detained personnel by the HUMINT agents of tactical Humint teams when they doubt the former may have information of intelligence value worthy of being exploited , conduct screening and interrogation on the spot in forward areas.Hence this screening results in the selection of persons having information of tactical,operational or strategic value.It is important to note that the CI agents must be very trained interrogators and linguists or supported by a trained efficient linguist team as screening and interrogation at forward areas cannot be compromised with time—time is of essence.We cannot afford to employ young untrained agents and neither the battlefield tactical situation warrants their training there.

NEED FOR INFORMATION OPERATIONS IN COIN – CENTER OF GRAVITY

The Prussian military strategist Clausewitz had coined the term ‘’Center of Gravity’’ with regard to any type of warfare. According to Clausewitz, an adversary’s center of gravity is in its concentration of mass. For our adversary , it can be any idea , capability , leadership association or environmental factor among other things that is critical in enabling it to be successful in its mission against us. This center of gravity , if identified and crippled can even destroy the enemy. One thing I teach in advanced Intelligence classes is what’s called “Center of Gravity”

In case of conventional warfare , the center of gravity requires kinetic attack such as war fighting to be destroyed. For example we might locate by aerial surveillance the command headquarters (tactical/operational) in the Area of ops and targeting it becomes the mission for our attack platforms as if it is crippled the enemy goes into disarray without proper command and control. In any battle scenario , there can be more than one or several critical points which we can term center of gravity. These nodes should be targeted first.

The case is totally different in COIN. Here it is highly probable that the center of gravity of the enemy lies within the population who are essentially non-combatants. Like the conventional enemy the insurgents too require combat support and combat service support. Now we must clearly understand that in an insurgency the number of insurgents is much less than the ‘’quantified’’ support it receives from the population(by quantified I mean the number of support variables operating in the area , the support roles) , both those who are openly operating in the villages and those who are actively supporting underground. Now as per Clausewitz center of gravity is where the greatest mass is located, so here the enemy’s concentration of mass is not the insurgents themselves but the support roles , that is the populace and now we just cant go on killing the population to effectively destroy there center of gravity. Hence killing is not the solution as now we are dealing essentially with non-combatants. One thing should be understood clearly. The security forces , the counter-insurgents presence among the population must have a clear defined objective satisfying the primary need of the populace. And that is the protection of the latter. Just merely being present among the community will not enable the security forces to get the support of the populace—this support is exactly the center of gravity of our security forces. A counterinsurgent’s goal is to protect the populace, therefore the greatest concentration of mass is going to be in these population centers.

We m must remember *the mere presence* of the security forces among the population is not sufficient to create conditions for seizing the center of gravity from the enemy or creating a center of gravity. Rather it is the *perceived reason* by the populace *why we are there*. to protect them .

Similarly the support extended to the insurgents by the same community is their center of gravity. Insurgents go to great lengths to gain the support of the locals. That ranges from extensive psychological operations/brainwashing such as indoctrination of insurgents ideals/policies/defaming the government/pointing out atrocities of local police and administration /promising rewards for information about the security forces/promising a better governance and resolution of land disputers etc before a martial court managed by the insurgents etc – in short an information warfare coupled with psychological tactics.

If our security forces have to turn the populations support in their favor thus creating center of gravity they must first disrupt the center of gravity of the insurgents—these very public support variables. In effect like the insurgents have bought the loyalty of the local tribes/communities/village heads/members of the panchayats similarly we must prove that our forces are there for the protection of the community and this is not enough , to seize and retain the center of gravity we must execute information operations , to offset the information and psychological operations of the insurgents. Then only we can disrupt and render ineffective their center of gravity , seize it from them , retain it and finally defeat the enemy.

The insurgents will of course resort to countermneasures.They will do everything possible ,mostly violent to disrupt the operations of the security forces so that they can highlight before the local community the failure of the security forces , thus passing a clear message about the ineffectiveness of the latter in protecting the communities/tribes. If this happens our forces lose the legitimacy they had gained by virtue of their center of gravity , and now as popular support is waning they find themselves on the receiving end , both from the insurgents and the populace. The latter now starts looking for alternatives to the security forces—the insurgents were already waiting and now the center of gravity shifts towards the insurgents. As population support starts going against our forces , we lose much ground which we had covered earlier.

HENCE THE COUNTERINSURGENTS MUST CLEARLY UNDERSTAND THE IMPORTANCE OF THE CENTER OF GRAVITY AND THAT IT NOT ONLY IS THE MOST EFFECTIVE WEAPON IN THEIR ARSENAL BUT ALSO MISSION CRITICAL.

Counterintelligence :Denial and Deception.Two powerful techniques of the enemy

Deception, denial, and other counterintelligence (CI) practices in 4th Generation Warfare

4th generation warfare is highly irregular, unconventional and decentralized in approach.

Asymmetrical operations are employed to bypass the superior military power of nation-states to attack and exploit vulnerable political, economic, population, and symbolic targets, thus demoralizing both government and its populace.

Both organization and operation are masked by deception, denial, stealth, and related techniques of intelligence and counterintelligence tradecraft. Enemy agents wear no uniforms and infiltrate into the populations of the nation-states they seek to attack.

Information age technologies profoundly influence terrorist organizations and operations. The development of network-based terrorist organizations with transnational connections through cell phones, fax machines, e-mail, and websites provide these non-state armed groups with global reach.

Modern communications and transportation technologies greatly complicate this new battlefield. *Not only are there no fronts, but also the old distinctions between civilian and military targets become generally irrelevant.*

Laws and conventions of war applied to nation-states do not constrain terrorists (and their state sponsors) as they seek new and innovative means, including the use of weapons of mass destruction, to attack civilians and nonmilitary targets and inflict terrible carnage.

4th generation warriors, frequently in the name of religious-based millenarian ideologies, are remorseless enemies. Their operations are marked by unlimited violence, unencumbered by compassion or constraints.

Deception Techniques used by enemy forces

One of the first steps in training terrorists is the assignment of a new identity. So significant use of false identities and proper documentation of it is very important.

There are specific sections that “specialize in obtaining travel documents for members who are deployed to foreign countries”.

Terrorists are also trained on how to use various covers that allowed them to blend into the location to which they were deployed.

Sleeper cells were used extensively to establish the operational infrastructure necessary for future surprise attacks.

Terrorists created business and other fronts that make it possible to raise funds to cover the terrorists' living expenses and for the purchase of weapons and bomb-making materials needed for a future operation.

Terrorists create covert cells and overt fronts for operations.

Terrorists were also obligated to perform duties they knew to be haram, forbidden by the laws and customs of Islam.Such as drinking liquor and resorting to lying.

Terrorist cells are compartmentalized. An operation is broken into two separate cells, the first performing infrastructure development, logistics, and operational planning. This cell conducts surveillance, tests target security, gathers intelligence, acquires the explosives, and constructs the bombs. Ideally, much of this transpires before the second cell is completely organized.

Terrorist operatives also encrypted files on computer systems in many different places.

There is speculation that, based on terrorist training manuals, operatives were instructed not to travel in groups and to use "secondary stations" to avoid detection.

Terrorists create a complex network of financial transactions by which they move hundreds of thousands of dollars.

The terrorists also mislead authorities by minimizing their associations with mosques known for their radical tendencies, though there are accounts of several hijackers visiting mosques during their U.S. stay.They also read namaz once instead of 5 times.

Terrorists sometimes use the mosques as places to communicate with other terrorist members and to exchange information as they believe that houses of worship were off limits to government agents.

A significant problem with many of the visas stemmed to terrorists is that not only from the hijackers' deception on the applications–including false or missing information–but also the negligence of the officials approving the visas.

<u>Some checklists for CI agents to follow</u>

Intelligence analysts must be able to distinguish between real signals indicating an attack, and "noise" which refers to irrelevant messages or those sent intentionally to deceive.

“Noise” never comes alone nor is irrelevant. True signals are “always embedded in the noise and irrelevance of false ones.

Preconceptions can lead to self-deception and also play a role in strategic surprise.

Tactical or technological innovation may impede an accurate assessment of intelligence.

Secrecy and trickery are core strategies followed by the enemy groups “to avoid detection at all costs when infiltrating any state.”

The enemy members are rarely conspicuous and well blend into society

Communications and transportation should not be overlooked as they can be highly deceptive.

When any enemy command is certain that a particular telephone [line] is being monitored, it can exploit it by providing information that misleads the CI department and benefits the work plan.

Enemy groups always have a security plan which is defined as “a set of coordinated, cohesive, and integrated measures that are related to a certain activity and designed to confuse and surprise the CI forces.”

” For the plan to succeed, they make it -1) “realistic and based on fact so it would be credible before and after the work,” and, 2) “coordinated, integrated, cohesive, and accurate, without any gaps, to provide [the impression of] a continuous and linked chain of events.

If the enemy is easily providing information about their commander as the mastermind that conceived, planned, trained, and executed the operation; they are certainly deceiving.

The operatives charged with executing an assassination, assault, kidnapping, or bombing are certainly trained in 1)Cleverness, canniness, and deception; 2) keeping secrets; and, 3) remaining unknown to the enemy.

GUERILLA/INSURGENT COUNTERINTELLIGENCE

AND

THE GOVERNMENT COUNTER-EFFORTS

INSURGENT COUNTERINTELLIGENCE

The leaders of an insurgent movement must constantly anticipate and be prepared to thwart efforts by established authority to acquire information about their organization and activities. It is known that the success of the Irish revolutionists was in direct relation to the operational achievements of their security chief, Michael Collins, who made it his job to know in advance what the British were going to do. His strategy relied on gaining direct, personal access to metropolitan police records.

He was so highly skilled and successful in his strategy that he was able to get the original of a report from the police of the districts. The thoroughness with which Collins worked his intelligence system enabled the I. R. A. to know what its enemy was thinking and often what the enemy proposed to do and on what information they based their action, and the identity of their sources.

This is counterintelligence activity. The importance of a sterling counterintelligence strategy is highlighted in a handbook prepared by an instructor of Castro's Sierra Maestra guerrillas, General Alberto Bayo. In his handbook, counterintelligence activity is thoroughly assessed in the questions and answers he devised for guerrillas. In his opinion a counterintelligence agent was of greater value than 50 machineguns as an agent could work among the security forces while providing feedback on their intelligence and plans.

The insurgent organization's counterintelligence and security program must be able to withstand the threats posed by established governmental authority as well as that represented by other multiple factors. The insurgent organization has many real and potential foes such as competitive dissident groups, the unilateral interests of third-country sponsors, sympathizers, and foes, and even disaffected members of its own organization. Information is vital and is the amour of the organization. It gains valuable information of those that seek to penetrate or compromise it. It must concern itself not only with an enemy's deliberate efforts but with contingencies of all kinds—some weak or careless act of an insurgent, an unannounced curfew or document check, the compromise of a courier, or a natural disaster.Public recognition is most desired by the leaders of an insurgency as they believe this would strengthen their cause and objectives. They use propaganda to promote themselves in large communities and hold public rallies. They prepare for and expect the backlash that accompanies these rallies as the urban police and security forces are usually out in their numbers and get copies of their flysheets and pamphlets. They do not hide in the shadows as they are eager to be heard and talked about in the market place. They further their “popularity” by claiming the achievements of competitive groups when these earn public approval. They turn failure to advantage if it can serve to arouse the sympathy of the people, and promoting their martyrs to the cause of freedom.

This is the insurgents' way of building its future and legacy by establishing abroad popular base. But there is a contradiction between the importance of security and this need for popularity as popularity would lead to infiltration of the ranks. Segmentation is practiced by separating overt from clandestine activities and minimizing the possibility of compromise for the secret cadres.

Because of the sensitive organizational knowledge held by an area coordinator, the fewer people who know his identity or even home address, the better his security and that of the groups for which he is responsible. "Street" and secret cells are established in both the city and the countryside but they are unaware of the identity of any member. Identities may be learnt only of those whose overt duties get their names into the papers. The identity of the secret coordinator is similarly unknown to the leader of a street cell; each is required to report separately to a central committee.

As protection against possible compromises among the secret cadres, cells have a limited number of persons in them which would enhance their mobility, reduce possible detection and strengthen the chain of command.

The recruits most time lack discipline and sometimes can be disruptive to the goals of the organization. Assessment of the suitability of the recruit is necessary and instructors are brought to the training camps to work with them.

The urgent task of a training cell coordinator is to satisfy himself about the reliability and resilience of a volunteer. He tries to learn as much as possible about the man during the few hours he has him under observation. Might he really be working for the government? In any case can one trust him with secrets? With money? Or the lives of others? What is his motivation? The assessment acts as a defense against penetration by any would-be police recruit.

Volunteers are thoroughly investigated and background checks are done to ensure their authenticity. The organization selects skilled individuals who use a variety of methods when conducting their investigations. Small talk, gossip would provide the investigator with good leads and indicators of the character of the recruit. Then the investigator will report to his superiors and intensify his inquiry. His search for information is no less thorough than that of government investigators and more comprehensive. The insurgent organization has more at stake.

Communication is the key element in any secret activity. If intercepted the adversary could successfully cripple the organization. For this reason an insurgent organization must have arrangements whereby the movements of funds, material, instructions, and reports are highly protected. Numerous methods, such as personal contact, mail, newspaper advertisements, and couriers are used to ensure that communication is protected and sent safely. The organization is vigilant in its safeguarding of its communication channels.

The use of codes and cover names are also used and these are frequently changed in order to reduce the chance of any penetration. These precautions serve the insurgents in keeping a step ahead of the police or any hostile force.

Insurgents generally avoid the use of mail for sensitive communications. They may send trivial messages by telephone or telegraph to signal the safe arrival of a member or to request a personal contact, but they prefer to keep in touch by courier. A courier can give reliable first-hand information as to the condition of his contact and can relay detailed instructions.

The insurgents often use drops for the transmission of funds, instructions, or material. These drops may not be sophisticated, they may be as innocent as using a hole in a tree. As long as it serves to conceal the act of communication, any method which both parties will have normal access will be suitable.

Controls over Cadres

Names and Identities

The insurgent organization, for its part, makes every effort to identify individual police officers, police informants, and hostile groups. It prepares lists of such individuals and informs its couriers and action units to avoid them. The organization prepares havens that are far away from areas that have security establishments. When there is a threat to one of its unit it would be instructed to move to that safe area. A courier is given the physical description of a security official operating on his route so that if he is caught he knows whether he is in the hands of security personnel or less dangerous adversaries.

Strict travel restrictions are usually imposed on the cadres and couriers. They are warned against carrying documents which conflict with agreed cover stories. Prior planning involves getting receipts of food or items bought in a particular area as confirmation that the courier had been there or belongs to that region. Avoiding detection and detention is critical so couriers must at all times look and act the part that they play.

Each member must know the movements and whereabouts of any other member of his unit. Any absence that cannot be explained or is considered suspicious is reported to the leader. Because it is known that each member is being watched and possibly reported on, members would tend to be more loyal and the unit is made secure.

The insurgent leaders have a constant concern that their members could be recruited by the police. They cannot object to a suspect covering his movements and engaging in evasive practices that they themselves taught him as good security.They must therefore refine their controls and devise tests to continuously assess his reliability.

The all-important thing is reliability and honesty. The insurgent organization thrives on suspicion which then causes discontent among members. This vicious cycle would generate the expected traitor and the leaders would establish new levels of severity which further disgruntle the membership. At the same time, however, these restrictions and controls do make the life of an agent who manages to penetrate the group both difficult and hazardous, and his case officer must have a thorough knowledge of the protective tactics used by the dissident leaders.

The insurgent takes measures to guard his camp or cell against those who come uninvited to the door. He extends a cautious welcome to any newcomer and examines the man's credentials with care. In the world of counterintelligence no one assumes he knows whom he is dealing with.

When camp sentries intercept a newcomer they follow a prearranged reception plan. They usually take him to a site removed from the main camp and thoroughly question him about his background, reason for coming there and any connections that he may have to any member in the camp.

Quick background checks are made with members of the command who might know the man. Clothing is given to the newcomer in exchange for what he wore. His clothes are checked for any evidence that can support who he says he is. The guards who live with him at the processing camp make every effort to get him to talk freely. They talk about the area he came from, question him concerning his likes and dislikes, and comment on true and fictional personalities in his home village.

Conversely, the guards avoid divulging anything that may provide valuable information about the organization to the man. They use their war names in conversation. They do not discuss other members of the group, their comings and goings, or their problems.The stranger is sent to another site while investigations continue into his background. As added precaution the camp is moved to a different location as it is considered compromised.

Should investigations reveal that the man should not be trusted the camp chief will use his discretion in deciding the treatment of the suspect.

A camp chief must always be alert and aware of his surroundings –are there neighbouring dissidents who may be under surveillance. He cannot afford to be caught in a counterinsurgency sweep even though he may not be the target. If there are scientists or researchers in the area they may report his presence to the authority. The locals can cause him some amount of inconvenience as they may gossip and the authority gets valuable information.

In anticipation of the eventualities alternative camp sites are prepared and ready for immediate disbanding of the group.

The Counterintelligence Organization

Prime responsibility for the success of the counterintelligence effort rests in the hands of the guerrilla chief and the area coordinator. The counterintelligence organization is responsible for the security of its personnel, assets, and activities. It has the resources to observe and report on hostile security organizations and competitive groups. It maintains appropriate records and isolates and interrogates hostile agents. Ordinary members of the organization are aware that there is a counterintelligence core but do not know the details of its make-up. The counterintelligence personnel are concealed from the rank and file.

The counterintelligence program usually includes lectures on security discipline, spot surveillance of personnel, and challenging tests of loyalty. Each cell appoints one of its members to the group who is then made responsible for enforcing the rules and reports violations to the cell chief.

It is of no surprise that the insurgent organization would be suspicious of members who have been recently released from prison. It immediately implements various security measures to protect itself from any likely threat that these members may cause.

Many changes are made in the organization that would invalidate any knowledge that the imprisoned member might have. Connections to colleagues are severed, his family may be sent to another location and there are internal investigations to analyze the details of his arrest.

There are established procedures that the newly released member must obey, such as he should not write or try to contact his group but proceed to a designated point at a time set for this purpose. He faces further interrogation from the counterintelligence specialists who try to determine if he has “turned” or should be trusted.

Knowledge of one’s enemy is power and the insurgency gathers this knowledge by placing its informants as servants in the homes of police officers, in police clubs, or with other hostile personalities. The value of such plants is obvious. They can get useful information from dinner conversations or by answering the telephone in the absence of their master or by monitoring his mail.

Money is another tool that is used by the insurgent to acquire informants. The insurgent organization does everything in its powers to counter espionage and disruptive efforts of opposing forces. All its efforts are designed to conceal and protect itself from hostile penetration. The strategy of counterintelligence - learning about the plans, personnel, operations, assets, and organization of its adversaries –is what is used to prepare itself to conquer its opponents.

THWARTING INSURGENT COUNTERINTELLIGENCE

Information is always vital to the counterintelligence officer as he seeks to identify insurgents. He exhausts all channels and clues that would generate even the slightest bit of information. The telephone directories, military files, surveillance and investigators' reports, even testimony from priests and professors, prove to be gold mines of information to the counterintelligence officer. Both hard facts and potentially useful bits of gossip, speculation and even criticism, help to form at least a sketch of the kind of person who may be an insurgent. The counterintelligence officer would be able to glean an understanding of what motivates this kind of person and what role and function he has in the organization.

The counterintelligence officer focuses his attention on the movements of the couriers of the insurgent organization. Couriers are usually in contact with persons who are at varying levels within the organization. Keen observation of the courier could provide insight into the insurgent's immediate plans. An even more important target for the counterintelligence officer are the area coordinators, because their knowledge of the organization's operation is accurate and at a high level. In-depth knowledge of the insurgent organization's physical and personnel assets can give some indication of its scope and operational prospects.

From interrogation reports the counterintelligence officer may get the location of safe sites abroad and the identities of foreign sympathizers. The counterintelligence officer is able to "connect the dots" within the insurgent's organization. Funding channels are discovered and political connections and influence are made more obvious to the counterintelligence officer.

With more solid information he can see clear patterns in incidents of bombing, kidnapping, assassination, and intimidation of police and private citizens. What are the results that the insurgent is trying to gain from such mayhem and confusion? Such incidents can provide indications of the imminence of larger, organized action.

The counterintelligence officer must securely, routinely and methodically record all the data and intelligence that he has uncovered. The information must be clearly constructed and stored so that it is easily understood and readily available when needed. All the details of persons who have come to his attention: their full name, alias if known, date and place of birth, address, occupation, and data pertinent to their dissident role, must be recorded in the file. His notes and cross-references must also be recorded in the file.

More expansive personality files, including the subject's military and educational history, strength and weaknesses of character, position in the insurgent organization, and relationships with comrades and associates, are also created. No detail should be omitted or considered irrelevant. These records are the counterintelligence officers working file, his tool for operations.

The established authority exercises its powers to control, restrain, or harass members of the insurgent organization. Without notice, the government can declare martial law and suspend constitutional guarantees. Such action would effectively deny the insurgents any opportunity to vent their views and draw attention to their movement.

Counterintelligence can also put added pressure on the insurgent organization by exploiting the arrest of individual members. Misleading press releases could be made to the public about the cooperation of some of the individuals with the police. This would immediately raise suspicion about the individuals and upon their release their friends will interrogate them—perhaps to the government's ultimate advantage.

By maligning the characters of individual leaders of the insurgency, further suspicion and discontent is generated within the lower levels of the insurgent organization. This can lead to a disruptive force within the organization that can potentially distract it as it tries to maintain its own control and focus. Suspicion can be intensified by counterintelligence if, for example, a police officer warmly greets this member in full view of his fellow dissidents. The target is then left to quell his friends' suspicions, to protest his ignorance of the reason for the greeting. And the target knows, even as he tries to protest his innocence, that a guerrilla can never explain having a friend who is the police.

The counterintelligence officer needs useful, accurate information that can only be gained from within the insurgent’s ranks. Daring plans are made to gain entry into the enemy’s ranks. The counterintelligence officer would arrange to get arrested with the insurgents so that he would be accepted as one of them. While in lock-up he would make suggestions about how to escape, tries to protect them and guide them in how they should conduct themselves during interrogation.

The other ways to gain inside sources would be to buy information from the hungriest member of the meanest cell. This person may rank very low on the information hierarchy but the counterintelligence officer must begin somewhere.

Another way would be to sponsor articles in the press which describe the destructive, harmful activities, and constant threat posed by the insurgent organization and incidentally point out gaps in what is known about it. Readers having knowledge in these particular areas are urged to write the author. This action might not produce immediate results of great value but it is a seed planted that can bear future fruits. For someday an insurgent, leafing through old newspapers may discover the article, if he ever finds himself in a situation which gives him little hope for the future, he may remember this invitation and act.

The counterintelligence effort can be considered successful when it gains willing defectors. In taking these steps a defector commits himself of his own volition as he takes time to develop or organize the information requested. A defector may not necessarily be a great prize in terms of what he can give – he may have resigned himself to recovering what he can by selling the past. But unexpected rewards can be gained from a public plea for information.

By constantly provoking and riling up discontent within the insurgent's organization, the counterintelligence officer can be hailed as the initiator of dissidence in the dissident organization. The counterintelligence officer's tactics cause the young guerrilla to second-guess his decision to join the insurgent. He is gradually discouraged by the constant denigration of its leadership, provocations against its members, publicity for its noxious activities, offers of rewards for information about it, and the ever-increasing controls and suspicion it promotes. In time the young guerrilla will want to leave -and counterintelligence would have won.

The value of a guerrilla who voluntarily offers his cooperation far outweighs that of the bought or seduced defector. Successful penetration of the dissidents' organization is dependent on the quality and trustworthiness of the agents that counterintelligence uses. The motivation of the agent must be understood and correctly aligned.

Selection of a potential agent is determined by such factors as their talents, employment location say a customs official, or a passport office employee. Such agents have to be briefed, prepared, and directed with the greatest care.

In a longer-term process, agents are selected to just hang around in the known areas where dissidents gather without making any positive approach to join them. The agents should frequent the coffee shops they patronize and act sympathetic to their beliefs. In the course of time, an agent would be approached and is offered to join their organization. The agent should neither jump at the first offer they make nor delay his assent too long.

Due to the fact that the insurgent organization is very diligent in screening uninvited persons who join their movement, the counterintelligence officer may choose to recruit a person already in place and avoid the hazards of trying to introduce an outsider.

The counterintelligence officer must choose wisely and carefully as his success will depend on how accurately he selects and assesses the candidate. Extensive and exhaustive study must be made of a candidate's dossier in order to assess his strengths and weaknesses, his desires and needs. Does the candidate have access to the desired information and, most importantly, can he be persuaded to cooperate.

Likely candidates can be found among dissidents who are under arrest. These candidates are most promising while still suffering from the trauma of arrest and before news of it reaches the public. The counterintelligence officer presents reasonable arguments and inducements to win the man's cooperation. He promises him freedom, immunity from prosecution for past offenses, and the prospect of a bright future. He can assure him that no one will know of his arrest or cooperation.

Usually, the prisoner is disoriented, in shock and distress while under arrest. This makes him a ready target for a sympathetic and understanding approach. He is more susceptible and easier to be persuaded to become an agent and assist the government.

Another method of defeating the insurgent is to create a phony guerrilla group in the mountains or the city. This would weaken the insurgent’s organization as its members would defect in droves. The decoy group would now be engineered and manipulated to be the new popular movement, while all its members in fact are being contained by the counterintelligence officer.

The counterintelligence officer has effectively created competition to the real insurgency, which cannot tolerate rival heroes, others' victories, and competitors for public favor. It must divert its effort and penetrate the new threat and bring all forces into its fold. This diversion can only weaken its real struggle against the government.

The counterintelligence officer is constantly doing battle against the insurgents with his provocations, harassments and infiltrations. All aimed to distract and keep the insurgents off-balance and fighting amongst themselves. He initiates action against it to disrupt a particular undertaking, exploit information received from agents, or unnerve his opponents.

These are the tools that are available to the counterintelligence officer. Violence is futile as the insurgent organization survives on it. And so the counterintelligence officer must use mental tactics, secrets and valuable information to control, exploit and hopefully eradicate the insurgent.

A carefully worked-out counterintelligence program is mundane and requires a lot of work. It produces no miracles but if given proper authority and power, it can yield great results in providing a harmonious society.

NOTE: The following points are the opinions of criminal (insurgents) regarding the security forces and the measures they undertake to escape detection and arrest

These involve those who have been employed from opposing groups. These groups cause maximum threat to the armed resistance movement.

Friendly (republican militant) intelligence needs to be constituted in a better manner and be more prepared as compared to the rivals. They need to be arranged into cells, where each party has restricted knowledge about the other, so that they are adequately protected.

Friendly agents and informers with good contacts should be situated at all communication and transportation channels and other organizational (trade union) and infrastructure administrative areas.

An analysis of enemy intelligence should be carried out to understand them from every aspect. This will enable them to secure their personal resources and exploit the weaknesses of the rivals.

As a key guiding principle, it was pointed that even though it was very easy to replace the fatalities from the enemy soldiers, the intelligence agents and spies who backed British efforts were very valuable resources and it would be very difficult or impossible to substitute them.

The IRA intelligence should give priority to recognizing important intelligence personnel at both the individual and group level whose loss would prove to be very damaging for them.

After enemy intelligence agents have been identified, they should be pressurized and forced to suspend their activities.

The police agents should be executed if they do not give in.

Those police and paramilitaries who indulge in criminal activities against the IRA personnel or support harsh measures should be eradicated even when the incident occurred a long time back.

Prior to the assassination, layouts, plans, timing and personal characteristics of the target should be thoroughly studied. This kind of extreme secretive assassination section also provided ways for getting rid of the weapons used.

To facilitate movement and reduce suspicion, individual members should encourage visual or other recognition with British or non-republican point of view.

It needs to be made certain that utmost confidentiality is maintained while enlisting.

Prevent individual guerrillas from becoming aware of the identities of more than a certain number of compatriots. Also, the knowledge about planning and organization, which is “an essential A-B-C of urban guerrilla security”, should be restricted.

It should be ensured that there is no negligence, indiscipline and lack of vigilance.

Documents, marginal notes addresses, telephone books biographical information, maps and planning materials should not be carried at any cost.

All the required information should be instilled in memory.

Those allies who infringe rules once should be corrected, however if they make these mistakes again, they should be punished.

Always be on the move and stay cautious so that police cannot identify the location.

Obtain information about police and security movement, activity and strength on a daily basis.

In the event of detention, security and silence needs to prevail, especially with respect to the identities or locations of the insurgents.

By and large, the most crucial lesson for guerrilla security regarding the prevailing threat is to never permit any violations in security measures nor show any negligence in their implementation.

Several CI reflections, in addition to particular treatments of the subjects that directly fall under the CI domain are interlinked through instructions and fundamental tradecraft. Some of these reflections have been discussed below, being essentially derived from *Military Studies* but also widely dealt with in other sources. These considerations are meant to determine the scope of the CI functions taken into account.

Keeping Secrets and Concealing

a. Information: The significance and challenges faced when protection information is considered, as well as using codes and ciphers. Through this practice, those who know operational details are prevented from sharing this knowledge, even with their spouse and closest colleagues.

b. Surveillance. Friends and foes are both considered as well as the different kinds and means employed. Several tradecraft topics which are linked to surveillance practices in different situations are also taken into account, for instance, becoming familiar with the area and target, flow of traffic, and the places where police stations and security centres are situated.

c. Recruiting, Evaluating and Training. This is a process that consists of several CI sensitivities; hence it receives the same amount of importance as several other insurgent groups. The *jihadist* recruit should possess the following characteristics: intelligence and vision, watchfulness and prudence, ability to survey, analyze, take action, change locations, and stay hidden, maturity, and the capacity to keep secrets. The different ways in which recruits can be “tested” for trustworthiness and competence are also considered, as well as the specific procedures through which agents who will be working for the sake of the movement will be enlisted.

d. Financial Security Precautions. The issues regarding handling and management of operational funds are also considered which include the requirement of keeping the location secret and preventing the safeguarding of money in a single location.

e. Protecting Documents, Forged and Real. This dimension pertains to the security of all documents and being completely familiar with them in case one encounters interrogation about the relevant documentations. In addition, there needs to be tradecraft-like strictures with respect to travelling to a country which allegedly issues the forged passport being used.

f. Care with Aliases. In those areas where operation is generally carried out, one should prevent having multiple identities. Also, the names of group members should be compatible.

g. Arrest and Interrogations. This pertains to the different kinds of interrogations as well as physical and psychological oppression which a *mujahid* might have to face. It also considers the different ways in which he should act in order to make the charge that he was tortured and demand that this fact be included in official records of his interrogation and imprisonment.

h. Security for Facilities from Infidel Surveillance and Actions. Safe houses and other facilities, mainly in urban localities, need to be carefully chosen. The selection entails appropriateness, entry and exit routes, as well as emergency escape routes and hidden places within these facilities which provide areas for hiding documents or other sensitive things.

i. Communications Security. This element pertains to giving attention to the means and risks associated with maintaining telephonic contact, conducting personal meetings, delivering information through messengers, letters, facsimile machine, wireless communications, TV and radio.

Defensive CI Practice

Insurgent forces make significant attempts in preventing the enemy [POLICE] from obtaining knowledge about its leadership, organization, support system, planning and location.

Cases:

Many important defensive CI concerns were presented by Carlos Revilla Arango in his significant article “Insurgent Counterintelligence”. Amongst these was the prevalent need to have compartmentalization, vigilance in enlistment, communications, and protection of identities, implementation of control over cadres and other important areas and creating identification with others.

Establishing agent networks, guarding information, (especially the recognition of guerrillas and attainment of rosters that the Japanese diligently looked for), securing different means of communication and short-listing of recruits.

Permitting the development of some kind of unexpected and unanticipated action which would have a negative impact on the operations.

Recognizing the spies and informants and handling them appropriately.

For example The Tupamaros Insurgent group were divided into cells which had two to six members, and each member in the group was not aware of the real identities of the other member (they referred to each other using “war names” or aliases). The leaders of each cell reported to a hierarchical leadership and they either had combatant/commando duties or support duties of different kinds. If a single member or leader was arrested and successfully questioned, there were little chances of the whole cell or even most of the members being detained. Cells of the “support” kind mainly dealt with intelligence matters, however, all constituents formed their personal contacts and sources, whatever their orientations were. This is also known a Compartmentation.

Recruiters depended on the personal contacts of the recruits, extensive application information and background checks with neighbours, friends and others. This would reduce chances of compromise by allowing informants to enter the structure.

The main objective of the intelligence organization of (Ex:Michael Collins IRA UK) was to gather important information using its vast network of well-located typists, clerks, businessmen, policemen, waiters, desk clerks, transportation workers and others who managed to obtain the most sensitive internal information from the British security along with other external information that was important too. There were limited technical ways of achieving this objective; however, they were all employed. Using this information, the Volunteers (IRA) operational force could attack and eradicate the intelligence forces as well as those personnel who played a vital role in the British intelligence-collecting process.

Every Volunteer organization had a devoted intelligence official who was managed by a brigade intelligence counterpart, an arrangement which made it possible to achieve this objective. The latter was headed by the official who was responsible for managing the daily activities at the Volunteer intelligence headquarters, which was supervised by Michael Collins. The intelligence HQ was also referred to as the “Brain Centre” and the main staff members were called the “Inner Circle”. The subordinate officials were responsible for hiring agents and informants who would provide information to the HQ which would be used in the targeted operations of important intelligence officials. The intelligence officials at the HQ were assigned particular business domains regarding which they had to collect information and analyze and also combine and analyze disjointed information.

Conclusions

There are variations in the guerrilla movements discussed here with respect to historical background, objectives, ideology, religion, race, resourcing and sophistication. However, majority of the groups have to work in an environment characterized by hostility and violence which means that the insurgent, regardless of his background, “lives in a world of security arrangements and survives by observing them” The insurgency is compelled by government intelligence and security measures to “carry out rigorous security examinations, rearrange components, relocate assets, alter its communications or re-educate its membership”. These are in addition to other actions which need constant supervision to ensure safety from any kind of disaster.

Even though the groups are distinct from each other in their nature and places of operation, when they face similar problems, they come up with analogous counterintelligence responses, as has been seen from the earliest of times. Such common ideas are executed because of the widely accessible information pertaining to the techniques, common sponsors and instructors from past and present and the examinations of the CI requirements by guerrilla groups.

There are both offensive and defensive elements of the counterintelligence responses of the guerrillas. Either of the elements is not perceived to be sufficient for granting the operational autonomy and security which is needed for engaging in active plans. With respect to the defensive element, extensive guidelines which address general conduct in addition to particular operational security requirements are sometimes formulated and added in recruitment and training sessions. Background and character assessment methods may be employed by the more experienced groups. These approaches might be as rigorous as the government security inspection or even more than that, provided the outcomes. Insurgent and terrorist groups are quite vigilant in securing their locations, abilities, methods of planning and objectives from existing and prospective opponents. In fact, some groups have become quite systemized in the practice of deception, cover story forgeries, forged papers, fake identities and several other tradecraft practices and use them proficiently.

Majority of the guerrilla organizations are constantly feeling the serious and sensitive threat of infiltration and treachery. In order to survive, these organizations need to conduct loyalty tests from time to time and also have vigilance approaching paranoia. European, Latin American, Asian, Middle Eastern and African groups provide rich examples, however, once informants or agents are identified, they are almost always executed during the process. In some groups, the punishment for treachery is very severe with the disloyal member being subjected to extreme torture and violence. These provide strong examples to others who might think about betraying. The security guidelines and processes are often kept as written documents. These guidelines serve as a means of training and reference for the guerrillas. At times, these serve as the norms of normal fraternal or social organizations which have incorporated huge doses of violence, fraud and uncompromising hate.

Guerrilla counterintelligence, in its most extreme form, seems to infiltrate susceptible areas of the government, military and police intelligence organizations, all of which are the offensive elements. They also include buying, blackmailing or forcing members, and sometimes targeting certain individuals or any other member and murdering them.

The historical approaches like the ones employed by Michael Collins eight decades ago appear to be ancient history, however, the approaches employed by Israeli Mossad against certain Islamic terrorist heads and those that are used by the terrorist groups themselves prominently exhibit similarity with respect to the process and method used.The jihadist literature especially stresses focused study and evaluation of military, government and police intelligence. However, guerrilla and terrorist groups, as well as organizations like criminal motorcycle gangs and animal rights supporters have made attempts to study and anticipate the methods employed by their opponents.

Targets on state intelligence and security agencies by the guerrillas may turn out to be a greater portion of insurgent activities. The safety of the terrorist and insurgent groups has become vulnerable and operational liberty is becoming more restricted because of the analytical tools, surveillance, interceptions abilities and, more broadly, the technological development of the government. Michael Collins supported with some success that eradicating an enemy intelligence official by force or assassination not only discourages the security forces, but it also develops greater disinclination amongst the population to oblige with the state agencies. When viewed from this angle, what the state or its residents rightly label as a terrorist act or cold-blooded execution may, in the guerrilla insurgent's view, actually be a "rational" counterespionage approach. An understanding of this perspective is important in addition to a complete comprehension of the objectives of guerrilla and the CI planning.

An evaluation of intelligence in war was carried out by Keegan more than 200 years ago. In his study, he found that the dispersed, networked insurgent/terrorist groups faced a lot of threat which made him believe that it would be productive to revert to the techniques "which have come to appear outdated, even ancient, in the age of satellite surveillance and computer description" for carrying out intelligence/counterintelligence missions. He found that there were benefits which could be obtained "only by returning to the oldest of all intelligence techniques, direct and personal counter-espionage" However, it is easier to support these ideas rather than execute them in a CI sense. These ideas are all excellent in a variety of ways and are reflected to some extent in the existing US military's stress on language and regional studies, culture intelligence programs, red-teaming methods, "human terrain system" development, and other attempts to encourage skills pertinent to human intelligence

These issues increase the intricacy of the CI “shadow battles”, as has been referred to by a particular specialist. Those insurgents and terrorists, who are recruited in counterintelligence areas, as well as all others, are aware of this and also understand it to some extent. Majority of the governments place a lot of importance on the technology gaps for intelligence and information management, however, in certain cases, there is a decrease in this gap, particularly for those groups who have access to hardware and software resources. Insurgent counterintelligence has successfully integrated the latest developments in time-based frameworks in the past few decades.

Even though “CI wisdom” has a long history of thousands of years, and has incorporated most of the modern developments, insurgents still face several drawbacks due to the continuous pressure. Most of the times, these are huge blunders because of which influential leaders are lost, as well as places of operations, important information, and other psychological setbacks. The insurgent CI mechanisms are deemed to be weak due to indiscipline and negligence, unpredictable morale, internal conflicts, worsening objectives, motivation (including criminalization) and pure bad luck as had been warned by Alberto Bayo almost 60 years back.

These blunders can be exploited by the counterinsurgent governments and spies, who can also develop them if they are well prepared and show perseverance, as is apparent from the history. Arango, a CIA officer, studied both the insurgent and the counterinsurgent CI issues and found out the approach which is most successful: active CI officers who possess carefully generated information and have constantly investigated their guerrilla opponents. They officers are aware of their ideology and tradecraft and carefully develop a CI plan of action, analytical drudgery and other hostile actions so that they can increase chances of insurgent failure. However, there is continual threat of those insurgent and terrorist CI plans that are based on analogous methods, have the same objectives and may be executed with a lot of effectiveness.

APPENDIX 1 CASE STUDIES

“Insurgency”, a word often confused as well as used with a near synonym “terrorism”. Although not very clear there exists a thin line of difference between the two. Often we see that the basic goals of both terrorists and insurgents are similar; yet if we examine insurgency and terrorism, specific differences emerge. The main base difference is that insurgency is a movement- an effort with a very specific aim and course of action. Another difference is the intent of the component activities and operations of insurgencies versus terrorism. Although there are places where terrorism, guerilla warfare, and criminal behavior all overlap, groups that are exclusively terrorist, or subordinate "wings" of insurgencies formed to specifically employ terror tactics, demonstrate clear differences in their objectives and operations.

The ultimate goal of an insurgency is to politically amputate the working power for control of all or a portion of a desired territory, or force political concessions in sharing political power. Insurgencies greatly require the active or tacit support of some portion of the population involved. External support, recognition or approval from other countries or political entities can be useful to insurgents, but is not generally aimed at. Whereas, a terror group does not require and rarely has the active support or even the sympathy of a large fraction of the population. While insurgents will frequently describe themselves as "insurgents" or "guerillas", terrorists will not refer to themselves as "terrorists" but describe them using military or political terminology as “freedom fighters”, “soldiers” or “activists”.

What can we guess the reason behind such risky moves? Obviously, there has to be a trigger factor for choosing such a path. If we look behind in world history, the most radical portions of the population are mostly engaged in such activities. Why so? Why would they leave the homely security and live lives of most wanted nomads? Yes, the answer lays in the brute fact that they have been denied justice time and again.

They were made to bear injustice that cannot be, has not been or will not be addressed by the so called governing power of varied countries. This very situation has mostly led the minority to take up arms in order to make the supreme power hear their pleas. But as times changed, the way and acuteness of their action changed. Starting from bow and arrow today they have successfully managed to outset violence with armed resistance. The core belief that led to these movements is that their cause is righteous (whether or not). In this era the belief has made such a strong foundation that based upon it they fuel the passions of general public. This sorry state could have been well avoided if the reason would be uprooted at the initial stage. Only if the existing situations would be resolved one could argue that no word called insurgency would ever exist. But sadly this was not done and the seeds have now sprouted to produce one of the greatest threats to not only general public, the government, a nation but the world peace at large.

Now if we examine the passion leading to insurgent movements in a deeper ground, we shall see that unlike conventional warfronts, they have the freedom of action. It becomes nearly impossible to predict their upcoming actions. They can make their own plan of action, at their own chosen times and places disregarding the conventional formulae. The upper hand they get is because of their geographic shelling and also some political organizations aiding them for transferring power from central to local control.

Further, they need not wait for permissions to be granted, rules to be passed, conventions to be maintained and other restrictions of statehood which may inhibit their adversary. Most importantly, their targets are specific, plan of action with unmatched convention and they have near-perfect intelligence which helps them to successfully prove their vulnerability.

Thus it is very well understood that the insurgency problems are not the branches of the terror tree that can be cleaned up by using brute force but it lies at the grass root level. Then what should be the way of approach to search and hit them? The answer lies in the question itself- i.e. handling the problem right from the base. Here comes into action the sensitive part of approach-counterinsurgency campaigns. These campaigns must be conducted with utmost discipline and vigor; and must incorporate all elements of national power into its strategy to have any hope of success. The methods used earlier had very little if not null effect in eradicating the problem. Although military operations are an essential component in counterinsurgency operations previous experiences have proved that political, economic and informational/diplomatic efforts ultimately lead to successful quelling an insurgency. One indispensable component of counterinsurgency warfare, which cuts across the entire spectrum of operations, is the requirement for actionable intelligence. Keeping in view the grounds of their action, only way to curb their encroachment is possession of a good intelligence, without which there is very little or no hope to defeat them. The successful management of counterinsurgency warfare depends on the well-organized intelligence architecture that is experienced, managed and carried upon. Given this fact, it is paramount that counterinsurgency forces gain this essential intelligence. Unlike the primitive conventions of war, counterintelligence does and does not at large depend on the data derivations from technical means (e.g. signal intelligence-SIGINT, imagery intelligence-IMINT and measurement intelligence- MASINT, respectively); but is dependent on collection of relevant information from human interface. This intelligence is harvested from the human intelligence (HUMINT), investigations and analytic capabilities of organic military intelligence and police forces in the area of operations.

Now let us have a deeper look at some case histories:

French Indochina: 1945-1954

Algeria: 1954-1962

Malaya: 1948-1960

French Indochina: 1945-1954

Overview: During World War II, “The Pacific War” by the Japanese, Vietnam was occupied by the Japanese, who took it from the French colonial government already there. After taking over Vietnam, the Japanese brutally enslaved the populace. This led to the resistance movement against the Japanese aided by the US on promise that Vietnam would be an independent country. Gradually the Japanese withdrew due to the A- Bomb; but the US went back on its promise and allowed France to retake its colony. The resistance movement then was called “Viet Minh” rebelled against French masters and the leader of the rebels Ho Chi Minh looked for new suppliers and adopted a more communist way of thinking and fought on, while his forces grew.

Analysis: As mentioned earlier there is always a catalyzing factor to these kinds of movements. Here too, the catalyst was the brutal torture firstly by the French and later on by the Japanese. But interestingly enough, both the French and the Japanese were defeated and colonies evacuated in spite of possession of much lesser freedom of action and development than their masters. Than what brought their success? What could have been the weakness of French and Japanese that were exploited for gaining freedom? Here lies the answer-

The French clearly lacked sufficient intelligence on the basic capabilities and intentions of the Viet Minh forces.

The underestimation of the Viet Minh power to fight back led to easy handling of their operational plans and troop disposition. Thus their mapping of plans could not be safeguarded from the enemy.

The prevailing historical accord of this war is that the French definitely lacked proper intelligence thereby trying to turn tables based on conventional style in counterinsurgency environment. By doing so they not only overextended their limited resources in an attempt to become supreme again but also found themselves chasing the wild goose ultimately gaining absolute nothingness.

Along with their failure to obtain actionable intelligence they also failed to maintain operational security the French dug their own graves and sealed their fate.

Conclusion: Definitely from the above analysis it becomes quite clear that the enemy possessed what the French did not. They had an edge in combat intelligence and hardly could the French ever guess what they were up to. The French had arms and power; Viet Minh forces had vast unbreakable underground intelligence collection network. For the French it resulted in expending their manpower and material loss thereby gaining nothing. Arrogance, inability to measure the depth of enemies, inexperience and lack of operational security and counterintelligence is what French forces possessed mainly. The intelligence web that Viet Minh forces created, aided them to be aware of even the slightest movement form their enemy side. Thus every time for a successful movement the speed of movement became necessary rather than its shelling. The Communist High Command therefore almost knew every little movement of the French troops in any sector and how many of those troops would be made available for those mobile operations. Thus is becomes quite clear that the visible lack of intelligence and their inability to safeguard their operational intelligence caused the downfall of the French in “French Indochina” war.

Algeria: 1954-1962

Overview: The Algerian War was a conflict between the French and Algerian. These were independence movements from 1954 to 1962 which led to Algeria gaining its independence from France after an important decolonization war. It was a complex conflict enveloping guerrilla warfare, marquis fighting, terrorism against civilians, the use of torture on both sides, and counter-terrorism operations by the French. Members of the National Liberation Front (FLN) on November 1, 1954 initiated this movement, the conflict shook the brass tacks of the French Fourth Republic (1946–58) and led to its ultimate collapse. The French Army initiated a battle of "pacification" of what was considered at the time to be a full part of France. The "public-order operation" rapidly turned to real war. Algerians, who had at first largely favored a peaceful resolution, turned increasingly toward the goal of independence, supported by Arab countries and, more generally, by worldwide opinion fueled by anti-colonialist ideas; but because of the volatility in France, the French Fourth Republic was dissolved. Even today this war has provided an important tactic casing for counter-insurgency thinkers, while the use of torture by the French Army has provoked a moral and political debate quite never to be resolved, on the legality and efficacy of such methods.

Analysis: At the initial stages the French were quite unfamiliar as well as unprepared for facing any insurgency movements. It was out of the box movement for the French and thereby they failed to face the enemy successfully. Hardly could they estimate the enemy power, path of action and available resources etc due to the lack of their own intelligence network. Whereas, the FLN intensely developed its intelligence network by then and the developed web constituted of maximum number of civilians. As a result of which working right under the noses of the French, they could be successful in slaughtering the enemy. Every movement made by the French was noticed by the guerilla columns infiltrating the colonized villages and unknown to the French information steadily flowed down to FLN leaders. Even when the French tried to develop their network, initially it was a hard nut to crack. They could not manage to collect reliable intelligence as the insurgents constituted of the rural population who enjoyed local terrain, complete freedom of action to strike back and withdraw unmolested.

French method of hitting the bull's eye: Jacques Émile *Massu*, a French general who fought in World War II, the First Indochina War, the Algerian War and the Suez crisis introduced an idea that would successfully stifle the growth and movement of FLN activists. The method constituted of constant patrolling and searching house to house and checkpoints in order to gather information as well as develop French intelligence network. Although Massu's method was worth it but most impressive was Roger Trinquier's-- a French Army officer during World War II, the First Indochina War and the Algerian War, serving mainly in airborne and Special forces units and also a Counter-insurgency theorist. He established a gridding system that divided the entire geographical area of action into symmetric blocks or grids. Then each large grid was again subdivided into smaller grids going down to the individual buildings and the families of French military units were assigned responsibilities for monitoring all the activities within the assigned grid. As a result of which surveillance became easier and successful to a great extent and information flow hiked up to a rapid pace. This method of gridding facilitated to build strong foothold within the community and build stronger relationships and as mentioned earlier the French army initiated the battle of "pacification"; this method was an important aspect for the effort. At the core level a small unit of Infantry Company who controlled a few villages developed sustained relationships with the inhabitants, developed trust and managed to include villagers who would work with the French in choking the rebels. These self defense units were called "harkas" who greatly helped the French to sort and destroy the rapidly popping heads of rebellions. Not only villages also the urban areas were included in the grid method where a "chief" was appointed to keep a close watch in his respective unit. To enhance the monitor identity cards were issued to each inhabitant. His job was to identify every living individual of the area and monitor the activities of each of them. Any unexpected, fowl activity was to be taken care of by him; and if he failed to do so he would be accused of helping the NLF. Although fruitful these methods visibly strangled the basic human rights and liberties. Yet for the good or bad the French managed to create forbidden zones, deploy Sections Administrative Specialists (SAS) and cleared some units resulting in nomadization. They organized effective police forces that shared the burden of the French officials and helped in penetration to hostile areas. Finally, by September 1957 FLN could be broken in Algiers.

Conclusion: Now if we consider both the cases in Vietnam and Algeria we clearly see that French used a method in Algeria that they failed to do so in Vietnam resulting in their downfall. Without effective intelligence even in Algeria it would be quite impossible for the French to continue their foothold. As diamond cuts diamond, here too without trickling down to the insurgency bed it would be impossible to create a loophole in the web of insurgency. To clear dirt away one has to get into it was the only effective policy that worked then and works till date. Since insurgents follow no formulae and convention direct interaction with the insurgents is the only way to know their plans and action. They have a well-knit family of activists who strongly believe to be fighting for their liberty, against suppression and for the good of their community; so they hardly betray their group under emotional floods or pressure. Gaining as well as keeping trust, changing their mindset to make them believe the authority can only help in checking their advancement. Thus finally quoting Colonel Roger Trinquier's view in order to enhance the fact discussed above, "*intelligence was one of several crucial enablers for defeating an insurgent. Others include a secure area to operate from, sources in the general population and government, maintaining the initiative, and careful management of propaganda".*

Malaya: 1948-1960

Overview: During 1940s the European community was well settled in Malaya. But by February 1948, communist guerillas attacked European settlers in the Malaya peninsula quite unaware of the British counter insurgency tactics of search and destroy. The insurgent units were nearly destroyed but the sudden death of the British High Commissioner again made a way for the communists to reinforce their activities. They applied every possible means to eradicate British settlement in their country-from convincing to killing the populace in order to achieve their target. But the British, very tactfully instituted the first helicopter in the "hearts-and-minds" campaign wherein they used helicopters to aid wounded civilians and military to the hospitals and provided necessary supplies and transport facilities. This "hearts-and minds" campaign was magically successful in contrast to the American method of using military power alone in Vietnam. Finally the Malayan communists fell apart after twelve years of campaign in 1960.

Analysis: Similar to the other two previous cases of Vietnam and Algeria, here too the insurgents maintained quite a similar base of approach. They kept themselves as isolated as possible from the government forces and kept creating menace time and again from different places and absurd times which followed no convention. T.E Lawrence's prescription "the first principle of guerrilla warfare is one of detachment from the enemy" was followed to the backbone by the insurgents even this time. Not only detachment, they also kept up with their second basic necessity of insurgency- "they acquired perfect intelligence of the enemy's movement and strength" though the means to acquire was both friendly and brutal. Here MPABA's political wing the Min Yuen developed an extreme network of informants and gathered relevant information about their enemy all the time. By doing so they always had a steady flow of information which allowed them to hideously develop their network and achieve success. But interestingly enough, the tables had turned this time. Insurgents were tackled with counter insurgency campaigns from the government's side. Now along with the military the local police forces were involved in handling the miscreants. Brigg's successor, General Sir Gerald Templer was the one to follow this method by early 1952 upon his assumption of directorship. It followed that the intelligence structure would be build around the local police forces mainly rather than the army as it would allow the intelligence net to penetrate deeper into the populace. As expected, this method enabled a more reliable and steady flow of information unlike the discrete flow faced earlier. With the development of this technique counter-insurgency began to flourish rapidly and the British undertook another effective decision of creating a well organized branch that would extensively deal with counter insurgency. It was a Special Branch of Police that dealt with the insurgents with a heavier hand than before. This group was responsible for proper collection and accumulation of the information which resulted in a beginning successful defeat of the insurgents. In order to assure services they began to mix need with patriotism; informers were being paid and some were even trained to act as double agents. This led to acute operations on insurgents resulting in capture cells after cells. With the improvement of this Special Branch even a school was developed which could train informers with the techniques to handle and derive information from and about the insurgents without leaving any trace of doubt to them.

END NOTE: 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 are designed.Personnel,physical and information—these three are critical assets and need to be fully secured against multidimensional threat intelligence collection efforts. Security education and training is inducted in the force with exactly this intent. The focus is primarily on the multidimensional threat intelligence collection efforts, the espionage threat and overall security threat factors. The soldier's awareness is heightened in these fields. The concept of insider-threat is also a major area of study.Terroism and insurgency is also dealt with. 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.

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.

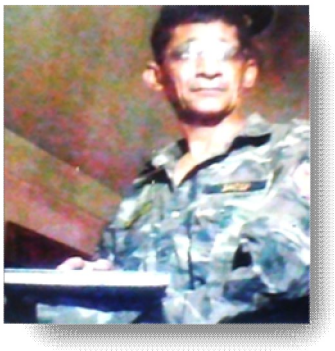
Intelligence Whatever be the divisions in function or overall structure , HUMINT and CI are indispensable to thwart enemy intelligence activities , to conduct force protection in a optimum manner,to keep our forces combat-ready to deliver precision strikes and to always keep the decision advantage in 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. The following are future enhanced capabilities to address the future environment and will aid in the execution of the UP *detect* function.

(***FOR TACTICAL HUMINT CONCEPT AND OPERATIONS PLEASE REFER TO THE HUMINT BOOK BY THE SAME AUTHOR.***)

There should exist knowledge centers pertaining to all HUMINT and CI acquired intelligence information at the theater , departmental and strategic levels.Data stored in this system will range from historical to near-imminent hostilities data. Included will be a separate future prediction (whether linear progression or nonlinear) section delivering warning data. Commanders , intelligence staff , operations staff and those with access permission to compartmentalized and classified information and a need-to-know clearance can access the data in these systems to satisfy their information requirements. Systems must be able to perform source and initial information analysis and have the communications capabilities to receive and pass data including digital imagery to analysts, consumers, and other HUMINT collectors in real-time and on the move.



Keshav Mazumdar DipCriminology,CPO,CRC,ASC,CMAS,ATO is engaged in intelligence/security activities and research and engaged at present in anti-terrorism research involving social network analysis, and exposure to intelligence-led policing, terrorist profiling, TACHUMINT,terrorist threat assessments and counterintelligence related security fields. He has his Antiterrorism Officer (ATO) credential from Institute of Safety & Intelligence, USA.He is at present the Sr Vice President ATAB,USA, Advisor (RIEAS) , Greece and also of European Intelligence Academy (EIA).He has been nominated to the Board of Geo Strategic Forecasting Corporation , USA.He holds a Diploma in Criminology from Stonebridge Associated College UK and in Criminal Profiling(INDIA).He is certified as a Master Antiterrorism Specialist by ATAB , Anti Sabotage Certified (ASC) by the College of Forensics Examiners International (ACFEI-USA),Certified Protection Officer by IFPO-USA and is a Certified Crisis Response Coordinator (CRC).In July 2012 he has been inducted as Fellow of New West minister College , British Columbia,Canada.He is a member in good standing of several professional Security organizations/Associations including the International Association of Counterterrorism and Security Professionals , Association of Certified Fraud Examiners, International Association of Bomb Technicians & Investigators, IAHN & the International Counterterrorism Officers Association. He is a registered member of the Int Association for the Study of Organized Crime. His has completed several NATO/Partnership for Peace courses, UNITAR Courses, and is specialized in threat and vulnerability analysis/assessment. He is a certified Human Resource Professional thus enabling him to effectively manage peoples and assignments. He has authored books on Intelligence, COIN, Warning Intelligence, Terrorist Interrogation and Antiterrorism. His expertise in unarmed combat is noteworthy--he is a regd. kungfu practitioner.

Along with Keith Flannigan Chair ATAB he is the administrator of two on line courses in Intelligence and Counterintelligence. This is an ATAB Endeavour to impart quality intelligence training to both Intelligence officers' as well as responders , a part of the course so designed so as to acquaint the latter with Terrorist indicators , pre-attack terrorist surveillance(dry runs),terrorist profiling and CARVER. The counterintelligence course also covers the TACHUMINT concept. The very important concept of I&W is dealt with thoroughly.

MEMBER OF:
International Assn of Counterterrorism & Security Professionals IACSP
INTERNATIONAL COUNTERTERRORISM OFFICERS ASSN ICTOA
International Assn of Hostage Negotiators IAHN
International Assn of Bomb Technicians
Antiterrorism Accreditation Board ATAB
Association of Certified Fraud Examiners ACFE
International Foundation of Protection Officers IFPO

HONORS/AWARDS/CREDENTIALS:
Anti terrorism Officer Credential ATO
Certified Master Anti-terrorism Specialist CMAS
Anti sabotage Certified ASC
Certified Protection Officer CPO
Crisis Response Coordinator CRC
Certified Human Resources Professional CHRP
Fellow of New Westminster College, British Columbia, Canada

He comes from a very respectable Indian family, his late father being a soldier and gentleman of highest integrity, war decorated Captain D.N.Mazumdar. He has strictly adhered to his father's principles. His mother and two sisters, both Professors have nurtured in him a high sense of respect for every living being, big or small, human or of the animal world. His belief in THE SUPREME is predicated by his feelings for mankind, for those in distress and poverty. But he is stoic enough to imbibe the true qualities of an antiterrorist, not flinching when meting out punishment to criminals/terrorists.

The below mentioned course site is offered only to VERIFIED Security personel around the Globe.

Intelligence/CI Course webpage


TIOCC
V CORPS
Intelligence Drives Operations