COMPANY LEVEL INTELLIGENCE CAPABILITY

June 4
2015

Proposal for fighting units of

Subject Matter Expert:

Keshav Mazumdar
ASC CRC CAS CMAS CPO ATO

Antiterrorism Officer
Sr Vice President,
Antiterrorism Accreditation Board USA

EXECUTIVE SUMMARY

Need for Company-internal intelligence gathering and targeting

EVOLUTION OF TACTICAL MILITARY INTELLIGENCE STRUCTURE

"No echelon has all the organic intelligence capabilities it needs to fully support
The commander. Commanders and Military Intelligence leaders at higher
Echelons should anticipate the intelligence needs of the lower echelons and
"Push" tailored intelligence support down to them."

Tactical units engage in combat with intelligence inputs coming from the MI dep't from higher echelons. In today's asymmetric war scenario the Company-level units should also have its own organic intelligence structures with very few personnel and assets deployed. They can act on available intelligence from the ground themselves without having to wait for collected, collated, analyzed information from Brigade Int section or other agencies which takes time—add to it the dissemination delays. In addition to conducting mission specific analysis and kinetic or non kinetic attack, the Company-level unit can also disseminate the intelligence acquired to subordinate units, parallel units or higher headquarters as these intelligence inputs may be useful to these parties as often intelligence about the enemy in one area of operations can help units in other operational areas, the enemy may be adopting similar tactics or other behavioral factors.

It is very important to recognize the lack of an intelligence structure at Company-level levels. The Company-level unit should have collection and analytical capabilities. There have been instances of lethal attacks on camps and bases itself-a force protection problem. We just cannot depend entirely on civil police and other intelligence agencies to supply us intelligence about the threat which usually is biased, and influenced by political and regional faction influences. The soldier on the ground who is a part of say the Infantry battalion engaging the insurgents , is face to face with the reality—the enemy , the local population and other parties of interest. Say during a reconnaissance patrol his team may come across a valuable source. After rapidly dismounting and ensuring he has no weapons, the teams intelligence component can start source cops like

Company-level or platoon level questioning, debriefing, etc and if a counterintelligence agent is also present the more the better for HUMINT collection.

Let us assume a Command (set up for COIN ops, or Antiterrorist ops in a State) which has everything in order such as Command chain, combat machinery, defined communication channels, civil administration support and police, civil intelligence agencies support lacks only an organic intelligence unit and depends on Higher HQ such as Battalion intelligence section and civil agencies for intelligence information.

It should be noted here that the necessary information is requisitioned first in the form of Request of Information document, which will go through various processing nodes as characterized by administrative channels, then finally landing in the collection manager's hands from the requested agencies higher authority to whom the request was directed. Now the collection manager will access already present records database and national databases to explore if the needed information is already available—if so he further initiates request for information, gets the information and passes it on to the commander of the unit. If not available he prioritizes the requested information as per the supported commands requirements, evaluates availability of suitable assets, allocates the assets tasking as per their capabilities, capacity and speciality,the assets are deployed, information collected, again sent up channels for evaluation of information quality , credibility (if source-submitted),analyzed, transformed into intelligence product and then finally disseminated to the supported commands commander.

All the above processes takes time, sometimes very long time, rendering the information useless as intelligence can at times be highly perishable, especially combat intelligence. The commander needs actionable intelligence fast and to enable this it would be far better if he himself has an organic modular intelligence unit, ready to take up assignments, if needed be integrated with the strike platoons itself for much faster information gathering and analysis and immediate action by the platoon commander. Company level/Platoon level intelligence capability can tremendously increase the competitive edge of the commander over the enemy, increase his situational awareness and be a force enabler.

Doctrine, Personnel, Training and Education, Leadership, Materiel Development, Organization, and Soldier Systems needs to be reviewed if intelligence assets need to be pushed down to the lowest level. There are dozens of units deployed in Company-level operations on the battlefield. If they are intelligence capable the Commander will get the best up-to-date and regularly updated(in the fluid war scenario of rapidly changing ground situations) intelligence inputs thus heightening his situational understanding immensely and thus giving him that decisive competitive edge over the enemy.

The need for projected intelligence capability is all the more important if the commander has to deploy to an unfamiliar area ,inhabited by an asymmetric threat which unlike a conventional enemy has no defined order of battle,organization,discernible patterns ,does not employ standard military tactics and where ops may be simultaneous , non-linear and distributed. In such a situation the commander needs to project his force by sending in interim combat enabled (for self defense) reconnaissance teams who have intelligence gathering ability as well as

counterintelligence asset , not the usual reconnaissance and surveillance patrols who are composed only of scouts and which do not answer the ‘’why’’ of things observed.

Today we are facing an enemy which is very unlike conventional adversaries who can be identified using intelligence as to their leadership,TOE,order of battle,strength,dispositions or anything which is determined by set doctrinal military tactics, techniques and procedures.Todays enemy in low intensity warfare is asymmetric in nature, taking refuge among the urban or rural community who act as enablers of the insurgent movement wither wholly or partially depending on the degree of acceptance of insurgent ideology and insurgent leaderships always try to influence the local communities to the maximum as they are well aware of the benefits of sanctuary among the latter. The enemy recruits, rests and reinforces/resupply itself from amongst the population. Here intelligence directly focused on the enemy is difficult in practice; the enemy is elusive, deceptive and resorts to unconventional attack modes and very adaptable but the enemy’s source of sustenance and very survival depends a great deal on the local populations support. The company and platoon sized units need immediate on scene intelligence support to deal with such a population enabled asymmetric enemy. As such even the smallest fighting unit must be capable of intense collection and analysis of information to get actionable intelligence instead of waiting for intelligence from higher headquarters which may entail time thus letting go of opportunities in combat. It is always not realistic to depend on higher echelon staff for intelligence. We must have an inbuilt intelligence capability in the smallest unit on the ground. The main criteria here is to shorten considerably the time between deciding on intelligence priorities ,detecting the enemy’s OB,Strength,disposition,capabilities and T&OE ,delivering the attack sequence and assessing the Battle damage and re-strike options.

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 meet ups 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:

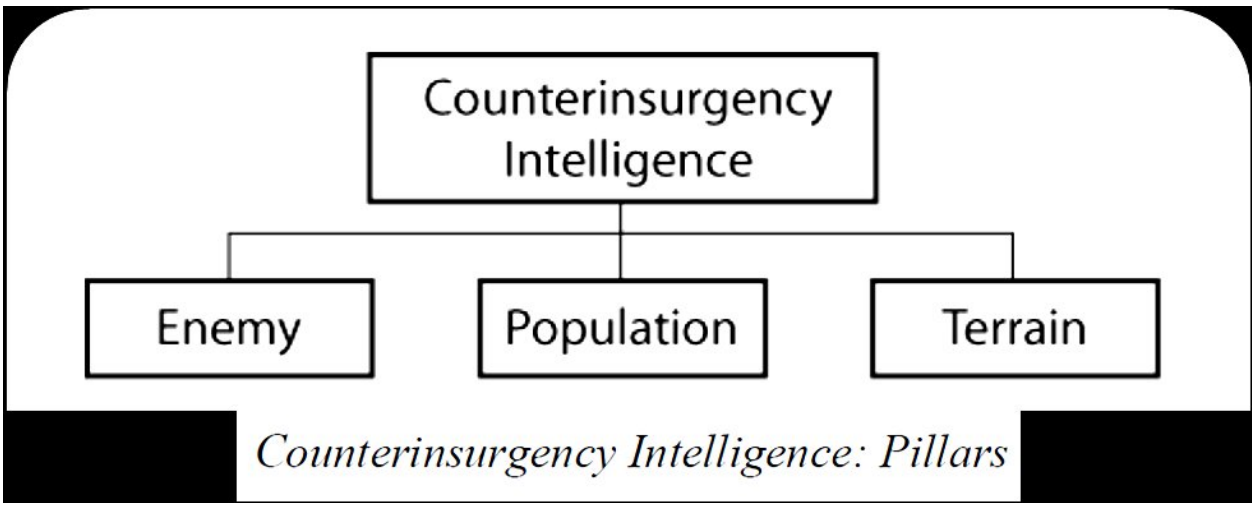
It is near impossible to allocate specialized intelligence assets to every operating force in the Area of Ops as such assets are few in number and the fact that majority of the information required for targeting flows ‘’bottom-up’ (that is the lowest level troops) necessitates the creation of intelligence 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.

Intelligence Requirements (PIRs) drive the military intelligence collection process.

While military intelligence officers help in developing intelligence requirements, it is the commander who is responsible for designating an intelligence requirement as a priority. The intelligence staff regularly updates the commander on its progress toward answering each PIR.speaking, that a military intelligence officer (STAFF INT OFFICER) and his staff are tasked with answering.
Additional intelligence requirements aimed at filling gaps in commanders' understanding of the operating environment and requests for information may come from higher echelons, lower echelons, and lateral organizations, or from the intelligence staff itself, but it is the PIRs that an STAFF INT OFFICER has been tasked with that are most important.
While emphasis shifts in various doctrinal publications, PIRs are generally supposed to2:
1. Ask a single question.
2. Be ranked in importance.
3. Be specific: Focus on a specific event, fact or activity.
4. Be tied to a single decision or planning task the commander has to make.
5. Provide a last time by which information is of value (LTIOV).
6. Be answerable using available assets and capabilities.

Usually, a commander only designates three to five intelligence requirements as PIRs at any one time.



Counterinsurgency Intelligence: Pillars

The PIR model makes use of intelligence-led and problem-oriented policing models that gained traction in combating crime in the United States after 11 September 2001 by refining them for practical use within the military dynamic. The recce unit along with the embedded HUMINT /CI element conducts area reconnaissance and community operations involving atmospherics, thus establishing a PIR framework before resorting to tactical questioning, elicitation and interrogation by using the PIRs to force conversations, gain community perspective and prepare

engagement summaries for analysis...The engagement summaries are analyzed, community feedbacks are compiled thus highlighting the causes that aid insurgency, enabling the unit in turn to recommend the targets that are the driving causes of the insurgency.

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

The Bn Intelligence section will consist of the Bn intelligence officer, a JCO , 2 havildars and 6 infantry soldiers. The Bn Intelligence section will interface between the companies and the Bde.The companies pass on intelligence information for processing to the Bn Intelligence section who in turn passes them on to the Bde and also as per ground requirements from the companies and Bn staff .The Bn intelligence section will develop sources and contacts from among the local population and liaise with the civil police and intelligence agencies. The question of deconfliction arises at this stage as the line companies and platoons have their sorces , contacts and liaisons as well as the civil agencies. It is the responsibility of the Bn intelligence section to deconflict its sources with all these sources, contacts and liaisons. The Bn intelligence section will use its HUMINT and other capabilities to detect weapons/explosives caches, collect incriminating evidentiary information for prosecution by the civil agencies and increase the overall situational understanding of the Bn and Bde commanders and staff. Delineation of sources between the Bn , the line companies , the platoons and the HUMINT units is very important by clearly defining the responsibilities of each with respect to the sources. We can have contacts like community leaders of influence , local politicians and councilors , surface and witting contacts as well as those contacts who are very useful , can supply information of rich intelligence value but need protection which will be the responsibility of the HUMINT units. The overt contacts like the community leaders etc can be the responsibility of the Bn intelligence section while the surface contacts and liaison can be given to the line units and platoons. The same line units and platoons can forward to HUMINT units any source of HUMINT interest which they come across community operations , patrolling or tactical operations.

Just like the Staff composition at Division level we can create similar structure at the Divn Bn level. There will be an Ops Staff officer and an Intelligence Staff officer. Compared to the Ops Staff officer the Int Staff officer, by virtue of his direct contact with the Div Staff Officer is better aware of all Div intelligence requirements, prioritized or otherwise and which requirements are tasked to subordinate units. His duties include analyzing collected information by Bn Int Section and effect the transfer of intelligence laterally and vertically, laterally to adjacent units , higher headquarters , line companies and even to the line platoon base camps. The Ops Staff officer will see to the tasking of Div intelligence requirements to all subordinate units.

To further push down the intelligence capability to the line companies level and platoon level , we can assign 2 NCOs at each line company and one soldier to take over as intelligence representative and co-located at the platoon level. During patrolling , reconnaissance by the Company soldiers , platoon soldiers , all collected information will be filtered , categorized and forwarded to the Bn Intelligence section for analysis and dissemination laterally and to higher headquarters. The intelligence soldiers at Company and Platoon levels can also requisition intelligence and imagery information from higher headquarters.

Secondary Collectors:
HUMINT collection is not limited only to HUMINT personnel. These can be termed primary collectors.HUMINT can also be and is collected (sometimes unknowingly and never reported) by secondary collectors like military police , troops and civil affairs personnel.

Take a scenario. A soldier comes across a man who offers information which the soldier feels could be of use to the HUMINT people. He does not bring the source in focus by detaining him or questioning him before others. He stays friendly , eliciting as much as possible after the source finishes his narration. He does all this discreetly. He manages to record the details of the source and when he is back from the check post to his camp he discreetly meets the Bn Int section officer and fills him up with all the information he has gatrhered.Therafter one and only one soldier in the Bn Int section passes on the information to the HUMINT operative with the contact details of the source.
In a second scenario the soldier may come across something , say a weapons cache , which he recognizes , and this exploitable intelligence he again passes on to the Bn Int section discreetly. In both cases he won't tell his colleagues or anyone. Thus we find line soldiers and other secondary collectors, if they keep their eyes and ears open, can create a good surface contacts base , thus reducing the workload on primary HUMINT collectors by gathering exploitable intelligence , the primary collectors can now focus on more important issues like prioritized intelligence requirements of the Commander. If all or many of the line soldiers or other secondary collectors work in this fashion the surface contacts base grows phenomenally, thus creating a secondary source base. Thus we achieve synchronization between primary and secondary collectors. The fact that the soldier does not tell any of his colleagues or even the chain of command renders the information to be exploited and away from any technical or influence detractors by limiting the sphere of knowledge. Further it is possible that any primary source may have links with the individual dealing with the secondary collector or any other link and this can be of value to the primary HUMINT collectors. Hence the bottom-line should be personal contact and liaison with the local community for every patrolling member.

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

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

Patrols, roadblocks, checkpoints, convoys—all these come into contact with enemy personnel (captured), civilians, civil suspects/detainees and criminal elements who can be subjected to tactical questioning. Hence the mission is to train the involved personnel in tactical questioning and integrate it in the planning and preparation/execution of the said activities. Pursuant to this prepare for debriefing after all personnel of patrols etc report to the unit intelligence officer

Prepare reports , verbally (debriefing) or written on any observations or information extracted after tactical questioning including being able to recognize any information of so much importance(combat intelligence) that it must be reported immediately without delay.

During such activities like patrolling, convoy etc all EPW/Detainee and seized documents must be subjected to exploitation carefully as these are prime sources of intelligence.

All the above should be predicated by the Unit intelligence officers tasking of prioritized intelligence requirements but collection outside these should not be ignored if such information is delivered by the source concerned. They might be of tactical value to the Commander or HUMINT officers.

Platoon Leader:

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

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

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

Company/Troop/Battery Commander:

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

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

Make it mandatory for everyone to be debriefed in keeping with the procedures laid down by higher headquarters intelligence staff.

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

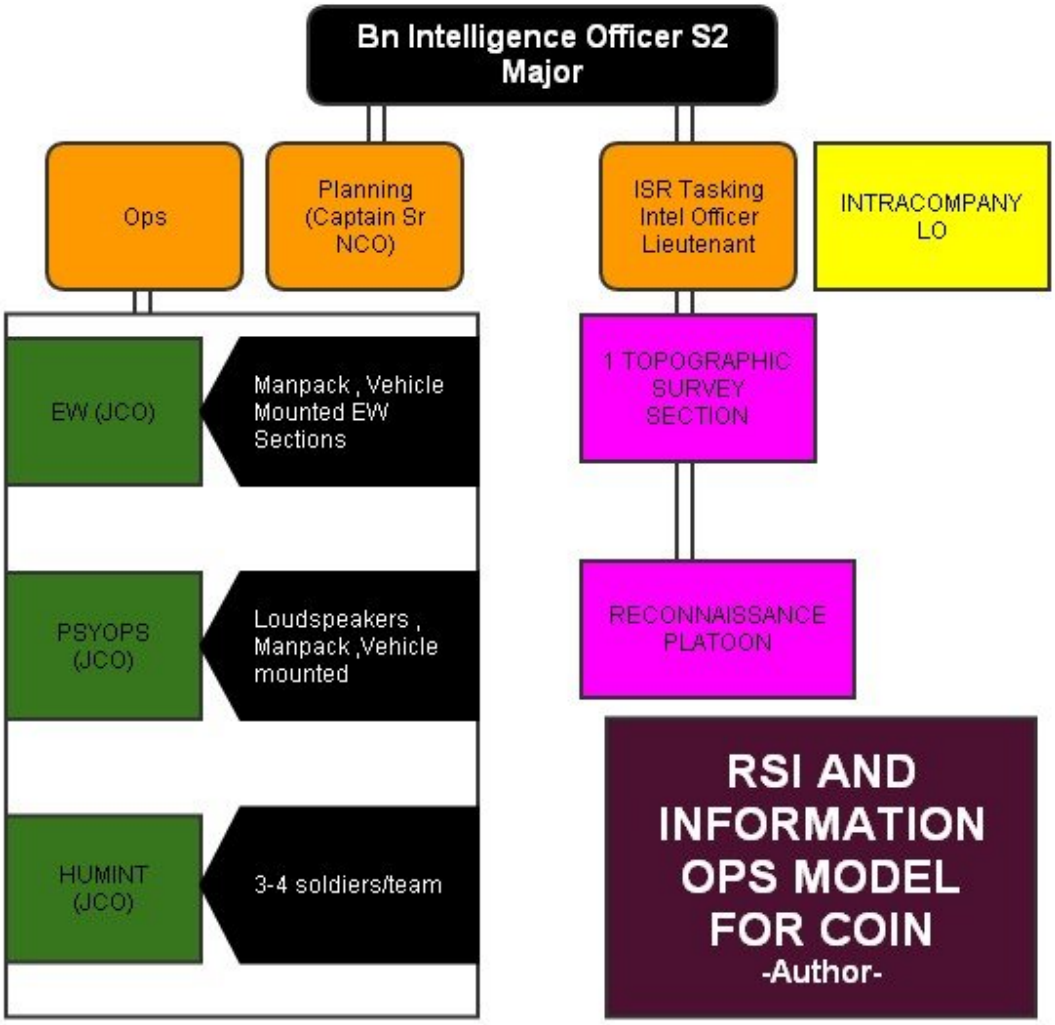
Battalion STAFF INT OFFICER and S3 Sections:

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

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

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

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



The fighting forces engaged directly with the enemy, companies and the platoons therein come into regular contact with the local communities, local administration, village heads and panchayats, and the enemy itself. The battalion may have its own intelligence section and if it does the section is very understaffed with one intelligence officer and an aide. The troops depend wholly on brigade intelligence inputs and intelligence feeds from other agencies. These inputs come as a result for requests for information from the ground and the process of requesting, tasking the request to brigade intelligence personnel, gathering the intelligence using collection platforms and pulling intelligence from adjacent headquarters, units and from national agencies and finally pushing it down to the combat team all takes time resulting in untimely intelligence feeds. Add to this the total lack of first hand contact of Brigade level intelligence section with the human and enemy terrain of the area of operations (human terrain is the local population) which is enjoyed by the troops on the ground fully. This lack of contact leads to low level of situational understanding of the higher headquarters and whatever

intelligence they gather is based on standard TTPs and intelligence sharing with other agencies. Yes certain cases involve infiltration by HUMINT/CI assets but as this is fraught with dangers and requires highly talented agents adept in deception and which is lacking in our intelligence headquarters intelligence acquisition using infiltration is scarce e are now left with the human terrain, the local populace and higher headquarters intelligence personnel will not commit to regular interaction with them like the soldiers on the ground do during patrols or securing an area after an operation or mopping up operations or during a cordon/search operation. Higher commands are not fully meeting their intelligence requirements of the companies and platoons in a timely manner; nor at the level of detail necessary for company commanders to successfully operate in the asymmetric defined battlespace.The company and platoon commanders must be able to portray the threat and disposition accurately nominate targets-both for kinetic and non-kinetic attacks and conduct successfully battle damage assessments so that the option of restrike does not get overlooked for example. For this is required a company level intelligence cell and pushing down further an intelligence enabled platoon. The infantry company requires and organic capability to collect, process, and disseminate intelligence to increase their operational effectiveness in full spectrum conflict. Infantry units require company level intelligence cells (CLIC) specifically organized, trained, and equipped to address this capability gap.

Each company (and in many cases several platoons) are assigned their own Area of Ops where the company level intelligence team or platoon level intelligence cell conduct intelligence collection activities and proper synchronization of ISR and integrating with the targeting process is invariably attained as all round collection involving the soldiers who are now the sensors leads to a far better situational understanding.

Primary tasks: Threat situation and disposition, Target nomination, BDA,Combat/security operations, surveillance, target acquisition, and reconnaissance.

The troops fighting on the ground are fed intelligence from Brigade level intelligence HQ.There are certain limitations which must be taken cognizant as well as the offered solutions (points 1,6 , highlight the need for company level intelligence structure)

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

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

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

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

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

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

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

Current asymmetric intelligence collection is the primary means to combat insurgency successfully by gaining a thorough situational understanding and developing first hand combat intelligence. This tactical environment needs our fighting troops to be trained in tactical intelligence collection to deal with an asymmetric enemy.
When a battalion is deployed, and usually stability and support operations are at battalion level we usually see that the battalion itself rarely executes its operation as a single unit. It devolves into sub-divisions which take up strategic areas in the overall area of operations. Detached posts/stations are set up in these strategic areas and these posts /sections create and maintain unit intelligence cells engaged in tactical intelligence collection on the enemy. Each garrison unit engages in low level source operations using standard intelligence collection methods, and getting a feel of communication routes.locational economics, topography and geography, human terrain intelligence and the political forces operating in the community together with any other criminal enterprises working hand in hand with the insurgent elements.

INTELLIGENCE PROJECTION CAPABILITY

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

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

The recce platoon, in addition to reconnaissance and surveillance should also engage in HUMINT activities for thorough situational understanding. The situation in asymmetric warfare is different. Here the recce platoon can conduct HUMINT operations. The reconnaissance platoon should be equipped with CI capability. This heightens its HUMNINT collection ability.

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

Military Intelligence Brigade

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

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

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

Brigade headquarters

- Ops Bn,
- Aerial exploitation/reconnaissance Bn
- Fwd collection Bn(CI/HUMINT) ,
- Fwd collection Bn (SIGINT),
- Comm. Bn.
- And electronics Bn,

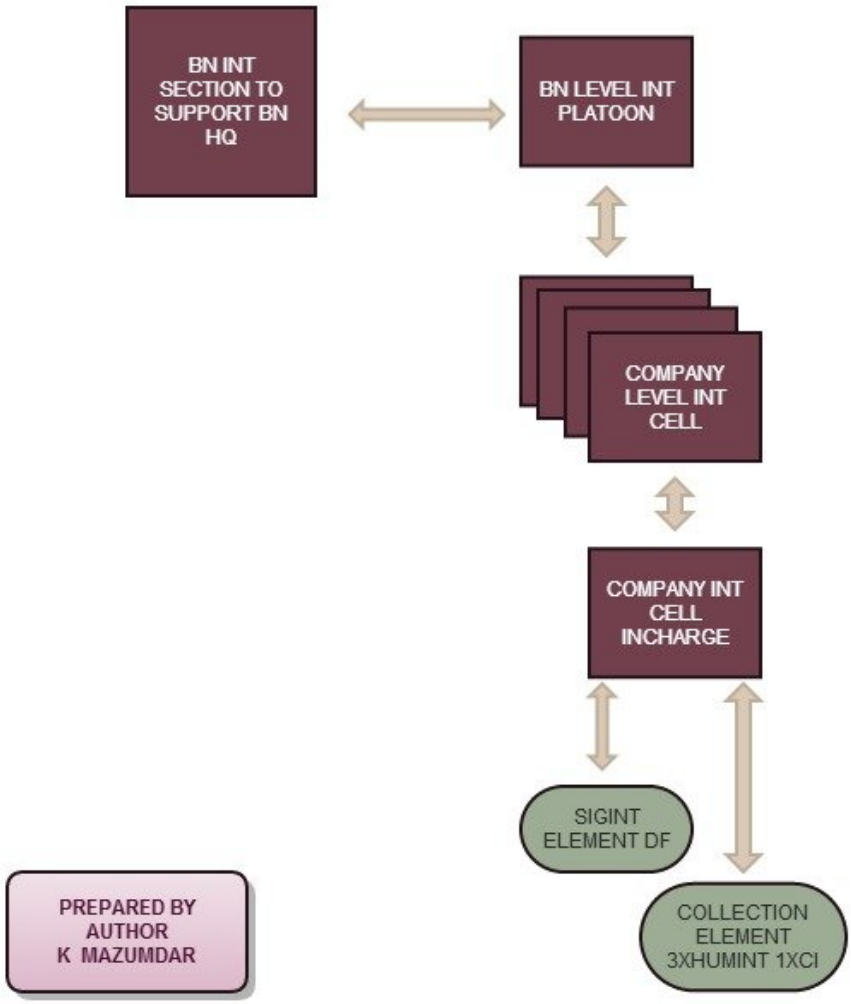


Figure 1: Bn Level Int Platoon comprising of Company level intelligence units

PUSHING DOWN INTELLIGENCE CAPABILITY FROM BRIGADE LEVEL

OPTION A: Military Intelligence (Ml) Battalion

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

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

The MI company in support provides-

- Communications intercept, direction finding (DF), and ECM.
- CI.
- Interrogation.
- Ground surveillance.

Personnel to staff the Intelligence Section, These soldiers conduct-

-Collection Management.

-All-source analysis and reporting.

-Dissemination.

-Technical control and tasking.

-Multidiscipline force protection and OPSEC support.

The TEB Unit provides

1. CI
2. interrogation of prisoners
3. ground-based SIGINT and EW support
4. and LRS support to corps operations

CLIC

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

There wil be two echelons in each platoon.

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

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

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

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

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

Company Level Intelligence Cells

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

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

Functions/responsibilities:

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

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

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

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

PROJECTING COMBAT POWER WITH ORGANIC ISR CAPABILITY

Reason for creation of interim team:

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

The recce platoon, in addition to reconnaissance and surveillance should also engage in HUMINT activities for thorough situational understanding. The situation in asymmetric warfare is different. Here the recce platoon can conduct HUMINT operations. The reconnaissance platoon should be equipped with CI capability. This heightens its HUMNINT collection ability.

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

C2:

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

HUMINT OR MI BN IDEA

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

Operations Battalion

Collection Management Section

Production Section ASPD & OB Teams

BDA & TGT Team

CI Team

Single Source Teams.

MASINT Team

SIGINT Team

HUMINT Team

IMINT Team

Corps Military Intelligence Support Element

Intelligence Support Elements

HUMINT Collection Operations

- Combating terrorism support
- Rear operations support
- Civil-military operations support
- OPSEC support
- Information operations support
- Civil disturbance support
- Local operational data collection
- Debriefing and interrogation
- HUMINT threat assessment

Reconnaissance HUMINT Missions

- Elicit information from the local populace.
- Interrogate EPWs and Detainees.
- Debrief Allies and U.S. personnel.
- Document exploitation.
- Threat vulnerability assessments.
- Source screening operations.
- Spotting/assessing for Tactical HUMINT Teams.

The early entry force, the interim combat team along with HUMINT/CI capability executes both an operational mission and intelligence endeavour.It shapes the battle space before the strike force moves in, makes conditions disadvantageous for the enemy in the initial stage , facilitates the arrival of the strike forces. It also conducts a preliminary intelligence preparation of the battlefield, makes a human terrain study and interacts with local populace using tactical questioning and elicitation to identify threats. In other words it helps in projecting the force into the new area of operations. In the case of asymmetric warfare projecting the force should be the case, not just deterrence. The latter part is force protection—is indeed very important, but if we have to uproot the enemy we need to be proactive, offensive and resort to projecting right into the heart of the enemy's base.

THE INTELLIGENCE ESTIMATE

Intelligence estimate. The intelligence estimate is derived from the intelligence preparation of the battlefield (lPB). It is based on all available intelligence and considers everything of operational significance. It will help point out gaps in the intelligence database. It is from these gaps that requirements are derived. It will provide information on the mission, *AO,* weather, terrain, enemy situation, enemy capabilities, and conclusions. It will cover all of the standard OB topics.

In the Army at the Division or higher HQ level the intelligence estimate is prepared by the Intelligence Officer and his staff...it is instrumental in devising the COAs by the Commander. The estimate sums up the intelligence factors affecting the mission. It identifies the enemy's probable COAs and the order of their adoption. It takes into account the Terrain and weather characteristics which might affect both the gauged intentions of the enemy and our mission and details the area of operations, the enemy situation and the capabilities of the enemy. The estimate is continually updated so as to keep the Commander abreast of any latest developments or changes in the intent of the enemy. This intelligence estimate is briefed at the Brigade/Battalion level. The intelligence estimate is predicated by the Intent of the enemy. Or Intents. The Staff Running Estimates helps each staff officer recognize and interpret the indicators of enemy intentions, objectives, combat effectiveness and potential enemy COA‟s which may counter the commanders end state. Thus the aim of the commander is to study the intents and devise appropriate course/s of actions taking into account several factors including order of battle, intelligence preparation of the battlefield, behavioral indicators, table of organization and

equipment, enemy capabilities and so on.(Order of Battle refers to the compilation of a systematic and methodical analysis of assets, capabilities, composition, and disposition of an adversarial organization, whereas TO&E refers to the organization table of units and associated equipment.)

To prepare this very important document the intelligence officer and his staff draw on the intelligence reports prepared earlier by the intelligence units detailing the terrain, weather characteristics and enemy strengths ,capabilities and limitations and the intelligence officer's conclusions about the total effects of the area of operations (AO) on friendly courses of action, the courses of action most likely to be adopted by the enemy, and the effects of exploitable enemy vulnerabilities. In other words ***we're conducting a CAPABILITIES BRIEF of the ENEMY Our MISSION is to develop an understanding of the ENEMY through the collection and analysis of available information, and then create an Intelligence product for dissemination.***

These intelligence feeds by the units upwards which aid finally in the preparation of the intelligence estimate, is the result of tasking handed down to the collectors/HUMINT personnel by the Collection Manager. It is here where the intelligence efforts of the HUMINT/collector agents come into play which is governed by the intelligence cycle.

OPTION B: COMPANY LEVEL MILITARY INTELLIGENCE CELL:

Organization

The MI cell (C& E), shown at Figure 2, is organized into a headquarters section, an MI unit (CI), an MI unit (interrogation and exploitation), and an MI unit (collection and exploitation). Headquarters section provides C2, administrative services, and logistic support for units of the company.

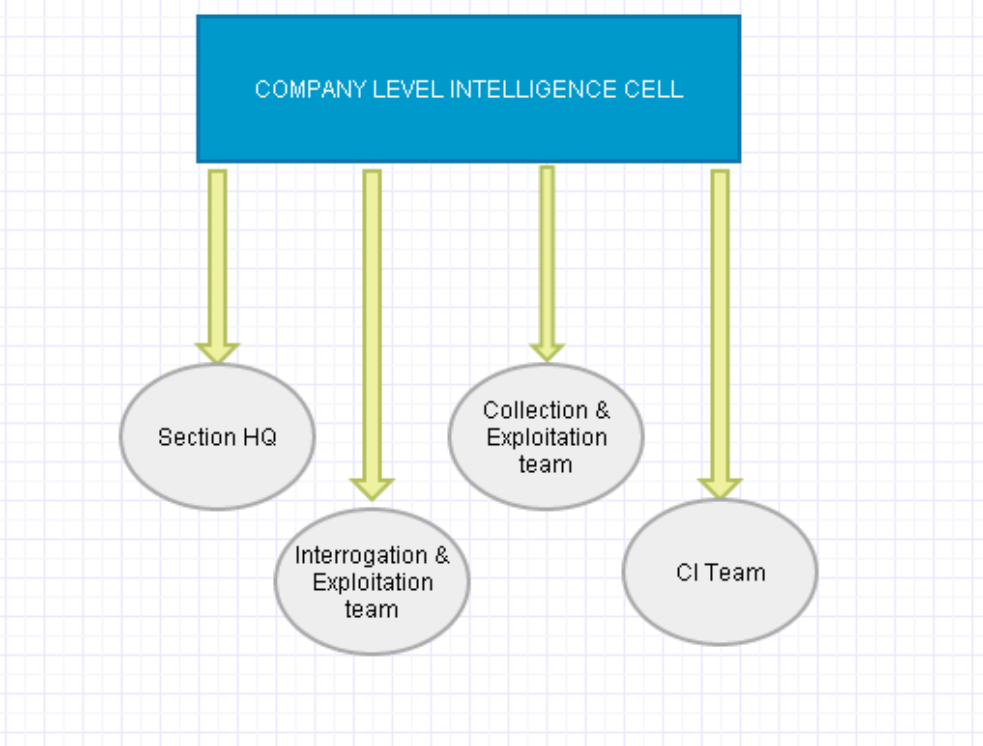


Figure 2: Company level Military Intelligence unit

Roles and Functions

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

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

MILITARY INTELLIGENCE UNIT (CI)

Mission

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

Organization

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

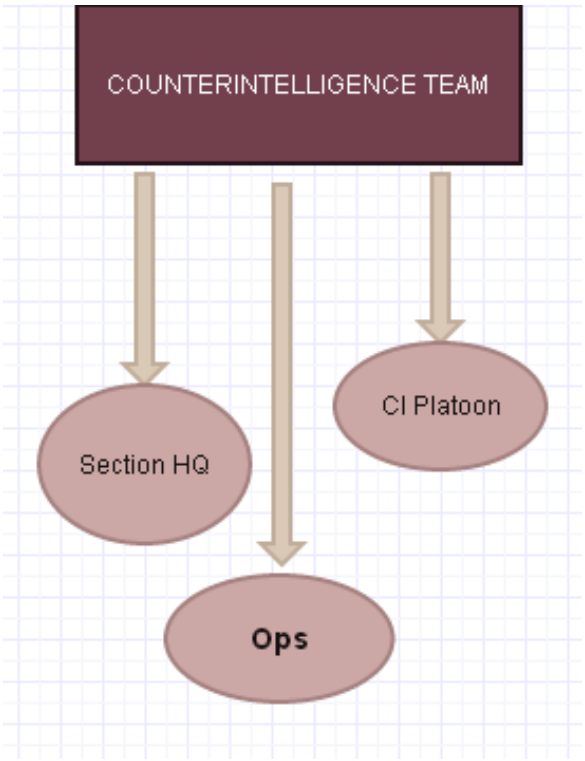


Figure 3: Counterintelligence Team

Roles and Functions

- Provides C-HUMINT support
- Conducts Vulnerability assessment
- Supports OPSEC
- Supports targeting , nominates HVT
- Conducts CI investigations
- Conducts Counterintelligence FP Source Operations
- Conducts counterespionage,countersubversion and countersabotage operations.
- Liases with other intelligence agencies
- Conducts offensive operations during wartime

Areas of interest:

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

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

MI UNIT (INTERROGATION AND EXPLOITATION I&E)

Mission

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

Organization

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

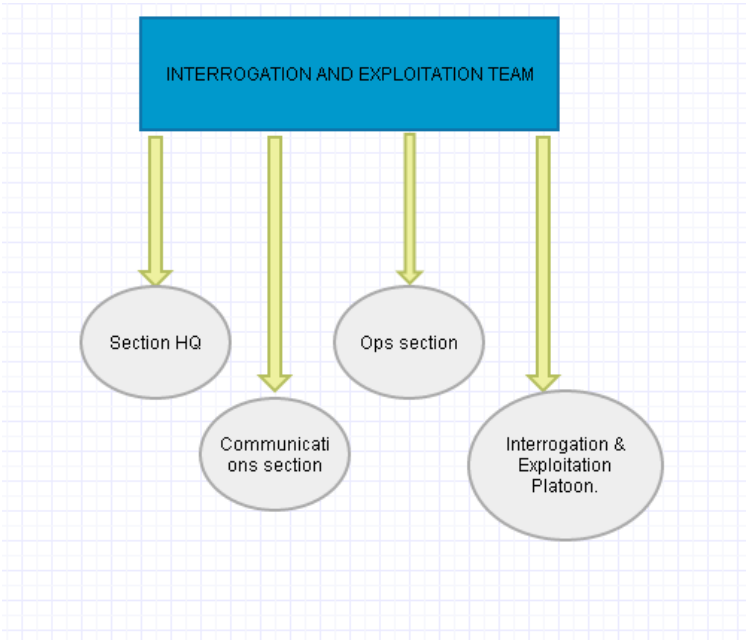


Figure 4: Interrogation and Exploitation Team

Roles and Functions

- ➢ Setting up interrogation facilities during wartime □

- Interrogation of EPWs.Establishment of a joint or combined interrogation facility and conduct interrogations of EPWs. Conduct debriefings of high level political and military personnel, civilian internees,refugees, displaced persons, and other non- US personnel.
- Conduct debriefing of high level military/political figures,refugees,patrols,military personnel who are released by enemy from capture or who have escaped from captivity,detained civilians and other people who have information of interest.
- Conducts DOCEX,and translation of captured documents.Translate and exploit documents acquired, found, or captured in the theater AO.
- Debrief US and Allied personnel having escaped after being captured or having evaded capture.
-

MI UNIT (COLLECTION AND EXPLOITATION C&E)

The above two units, viz MI (CI) and MI(I&E) are combined into one UNIT , collection and exploitation MI(C&E) and hence executes all the functions which are inherent in the 2 units. This is a modular unit, can hence plug as a detachment support into any Battalion/Company which requires CI/HUMINT support but does not require a full intelligence battalion /Company expertise. It can also be situation may not allow the deployment of full intelligence assets –in such a case the MI(C&E) can be scaled and tailored to suit the requirements of the Battalion. This unit can pull operatives from both the MI (CI) and MI (I&E) to create CI and I&E platoons to conduct tactical HUMINT (CI/HUMINT) missions with the available CI, collection, and exploitation and interrogation expertise.

Mission

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

Organization

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

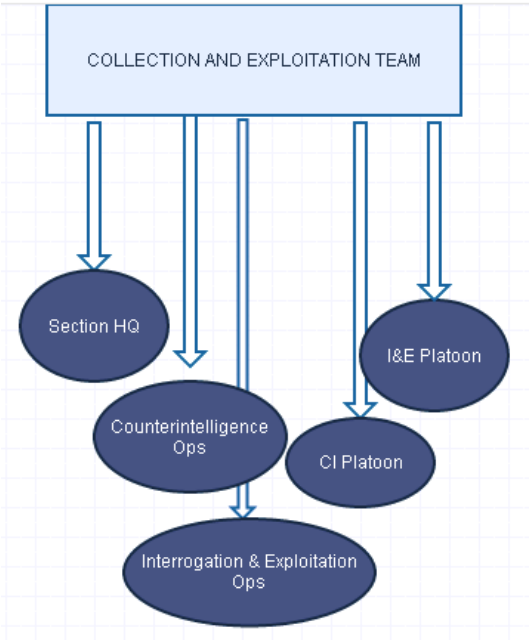


Figure 5: Collection and Exploitation team.

Roles and Functions

- Provides C-HUMINT support
- Conducts Vulnerability assessment
- Supports OPSEC
- Supports targeting , nominates HVT
- Conducts CI investigations
- Conducts Counterintelligence FP Source Operations
- Conducts counterespionage,countersubversion and countersabotage operations.
- Liases with other intelligence agencies
- Conducts offensive operations during wartime
- Areas of interest:
- Known or suspected acts of treason,sedition,espionage by Army personnel
- Known or suspected association with elements of threat intelligence
- Terrorism,assassination incidents
- Defections and unexplained absence of Army personnel
- People impersonating as military intelligence personnel.
- Setting up interrogation facilities during wartime
- Interrogation of EPWs.Establishment of a joint or combined interrogation facility and conduct interrogations of EPWs. Conduct debriefings of high level political and military personnel, civilian internees,refugees, displaced persons, and other non- US personnel.
- Conduct debriefing of high level military/political figures,refugees,patrols,military personnel who are released by enemy from capture or who have escaped from captivity,detained civilians and other people who have information of interest.

- Conducts DOCEX,and translation of captured documents.Translate and exploit documents acquired, found, or captured in the theater AO.
- Debrief US and Allied personnel having escaped after being captured or having evaded capture.

Areas of interest:

- Known or suspected acts of treason,sedition,espionage by Army personnel
- Known or suspected association with elements of threat intelligence
- Terrorism,assassination incidents
- Defections and unexplained absence of Army personnel
- People impersonating as military intelligence personnel.

DERIVATION FROM ABOVE →..

1.MODULAR FORCE DESIGN : The resources and capabilities at the hands of the Commander with respect to intelligence assets are limited , sometimes scarce .From the above we can introduce the concept of ‘’Modularity’’ in force design. That is to say we can create a deployable, scalable, modular intelligence capability to plug into the requirements interface of any adjacent unit/company/headquarters who lack the necessary intelligence capability or whose resources are very limited. This modular plug-in can be tailored to suit the needs of the Commander of that unit. For example if HUMINT assets are more in demand than the CI or DOCEX elements , the former can be augmented to the plug-in by pulling from the parent units MI Company’s sub-components , with the Company’s capabilities not being reduced in any way. The MI (C&E) is a good example of a plug-in.

2. Tactical HUMINT team formed at company level from CI and I&E platoons of the C&E Company.(Please refer to the Appendix for further details on Tactical HUMINT.)

Production Section

The all source production and dissemination team (ASPD) in concert with the Order of Battle (OB) Team, determines if intelligence requirements and RFIs can be satisfied with its existing information and data base holdings. Information not available defines the collection requirements. The collection manager then tasks collection assets within theater or requests support from national level assets. These two teams determine what enemy information is available to help identify specific indicators of enemy intent and provide a current, integrated picture of the battle space. During the analysis and production portion of the intelligence cycle, the ASPD and OB teams coordinate with and receive information from the other production section teams. This constant exchange of information ensures single discipline reporting is fused into all- source products.

BDA & TGT Team

BDA and targeting team (TGT) performs target development selection and assessment. Based on collected all source intelligence, the team identifies target vulnerabilities, provides targeting data and nominates targets in accordance with the commander's HPT lists and the attack guidance matrix (AGM). The BDA/ TGT will also assess battle damage based on physical damage sustained by the target and their remaining combat effectiveness

.

CI Team

The Counterintelligence Team performs CI analysis. The team assesses the adversary's intelligence collection capabilities and operations directed against friendly forces, missions, and installations. The adversary uses many methods to collect information against friendly forces, including HUMINT, SIGINT, and IMINT. As a result, the CI analytical capability includes a diverse mix of specialists who fuse information to identify and isolate collection operations. The CI team and other elements of the production section exchange critical information required to analyze the enemy. Intelligence gaps and lack of holdings are provided to the CM section for action as appropriate. Specific functions of the CI team include:

- Develops and maintains CI data bases.
- Monitors CI collection efforts.
- Produces IPB products to support CI operations.
- Produces analytical products, including threat assessments, estimates and summaries,threat situation overlays, and black, white, and gray lists.

INTELLIGENCE SUPPORT TO COMPANY

The targeting process is the culmination of another involved process, beginning from sensor collection activities, sent higher up to the intelligence section where collation, analysis is done, the finished intelligence product now being routed for dissemination to the targeting platform. Information flow is from down-up preceded by request for information from the troop level. All this entails time and intelligence is perishable, in that it is needed to be not only accurate and specific but also timely. To avoid this time delay or to put it this way: to reduce the time between sensor collection to targeting, we need to distill the targeting process down to the company or platoon level. If collation and analysis can be pushed down to that level, a great deal of enhancement in situational awareness and operational efficiency would result. One of the most effective of these was the distillation of the targeting process into a Troop/Company-level tool.

We can have a Company intelligence support cell which will help in the creation of Company and platoon level intelligence teams or grant assistance to units who have no organic intelligence capability.

The squads or platoons at ground level usually accost the enemy in rapidly changing environments with the element of surprise against them. In such situations the soldiers have to adapt real fast and there is no time for sending information requests to Bn Intelligence officer or higher up and waiting for intelligence...timely specific and accurate intelligence that is. Here ‘’timely intelligence’’ is crucial. Troops on most occasions find themselves operating unilaterally against insurgents conducting IDF, DF and IED attacks and have to adapt quickly. It is here that the intermediate level Company intelligence support cell can help by creating a squad targeting process by supporting the squads with raw operational intelligence by fielding its HUMINT and CI assets with the squad itself. Later it will be detailed how the HUMINT and CI enabled platoons are formed with the CLIC in the lead.

In the absence of the CLIC the usual intelligence summary report briefed to the Bn and Bde commanders omits the ground critical information need of the squad/platoon. The picture usually presented takes into account the operational success/failures as a whole and dwells on the priority intelligence requirements, not the immediate intelligence requirements of the tactical unit on the ground involved in combat. But if we have the CLIC setup, then the CLIC can increase the situational awareness at higher levels by sending in intelligence reports through the lens of the squad firefight.

SIGINT resources required to conduct effective personality-centric targeting are not available at the Company or Troop level.

All the information collected at the troops level is exploited where proper categorization and collation is executed. It is at the exploitation stage that the soldiers work is evaluated and decided who needs further training to collect information properly. Because the correct manner of collection of information is very important at the troop level. It must be duly ensured that he has properly conducted tactical exploitation of the area , of the captured materials, and of the human terrain. It must be seen to it that his knowledge of tactical questioning is thorough. All these performance indexes are reflected when the platoon intelligence unit or company intelligence unit submits their intelligence reports. This exploitation phase will require a great deal of administrative functions to assess the soldier's capability and also to assist in the collation of all collected information. Although at this phase nothing strong is produced against the insurgents, but further operations tend to be driven with the collected intelligence. This is where the Bn Intelligence officer or the Company intelligence officer decides on the technical control aspects of the collection being done by line soldiers and ensuring that they adhere to it now and in the future.

It can very well be that the projecting intelligence capability option is used where it is not practicable for having own intelligence unit. There can be the Company intelligence support unit/s, modular and available to all the Companies operating in the area of operations. These units can for example debrief returning patrols of the company. Returning patrols are a very important source of intelligence—this fact should be understood clearly. Now just coming and telling the Platoon section headquarters or the Company headquarters intelligence officer what information they have will not suffice the purpose. This information needs to be sent to higher echelons and that too systematically after being entered into the Company's knowledge management system, collated and analyzed. It is not that difficult as a computer system can be set up and today dozens of map tracking or link analysis softwares are available together with database management system software for small units.

The debriefs of the patrols should include what they have observed about the local population – any changes from earlier situations perhaps?—pictures taken, any information to satisfy the units intelligence requirements, any engagements with the enemy and if so where, any information from any civilian upon being questioned etc etc.

One thing that can and should be incorporated in a COIN environment is the ground level or company level intelligence units biometric collection and exploitation capability. If the soldiers can properly take DNA samples from members of the population enrolled in a DNA collection scheme and then all biometric information recorded in the database, in any future case of insurgent attacks all biometric evidence can then be cross-referenced with that contained in the database , thus if there are matches insurgent personalities get i9dentified , driving further operations , kinetic or arrest and prosecution.

Analyze

In this phase the Company intelligence support teams will study all information submitted by patrols (HUMINT reports), by special forces who went on raids , by forces returning from encounters with captured material and spot intelligence from EPWs etc , sort them and then study how they are reflected in earlier Bde or Bn intelligence summaries , to find out common information. This step is different than most intelligence analysis steps generally used in INDIAs COIN operations. We have cases like Dantewada or several cases of ambush. If the company intelligence support teams find that there exist past reports of ambushes and IED activity similar to the current patrols debrief and located in or near specific areas of the area of operations then a pattern emerges , indicating for example insurgent concentration points or say the terrain in these areas are conducive for ambush or IED placement. Or it can also mean that whenever our forces are visiting those areas they are being ambushed or IEDed so that they do not reach certain areas in close proximity which could be the insurgents operational headquarters or anything important for their operations or maybe containing population who are sympathetic to their cause, and whose questioning or area search may yield intelligence vital to the success of the forces and detrimental to the insurgents. Hence from the force protection perspective, finding reflections in intelligence summaries of higher headquarters is something the company intelligence unit gives high importance. Reflections will also help the Commander to make an idea about the effectiveness of patrols as any desirable effect on the insurgents, like capture, or increased movements or a spike in the behavior of certain elements/groups in the local population paves the way for further patrolling and enabling the Commander to act more decisively.

Disseminate

This phase is perhaps the most difficult one and also the most important one in that after the present company/s toil for a year collecting and maintaining intelligence information, relief troops need to be filled in with that information properly and it is vitally important that the Bn, company and lower levels need to be disseminated all pertinent intelligence in time , maintaining specificity , accuracy and timeliness. Thus dissemination is the most important part of the targeting process and how that information is utilized. The relief units coming in and being disseminated properly enables continuity in operations. Any break in this continuity is an advantage for the insurgents in that they get time to regroup etc while the relief company's are consolidating or trying to consolidate their position with little information from the departing units.

During dissemination the usual recourse is to pinpoint grid locations on a map where caches are located , or have been found and where encounters have been experienced or probable areas for encounter. This is not the correct way. Efforts should be made with the help of software or reasoning that ''linkages'' are established between these points. So that a larger picture of the area of operations results with interconnecting nodes.Say we have a local village panchayats house located a few blocks away from a madrasa which information collected shows it to be a

school for insurgents , being indoctrinated at night. Further some patrols have pointed out that in other areas around the madrasa there have been few arrests at evening times by the local police. Thus we find layers of intelligence makes the entire area involving the mosque and the adjoining areas very important from the security point of view. Then one fine day on doubt the panchayat leader was detained for an hour. Keeping the security importance of the madrasa in perspective—it as the threat—then we can extrapolate further and associate the panchayat leader with the madrasa activities and all activities near the madrasa under the scanner (the panchayat leader is a locally powerful man and happenings in a madrasa near his place of living cannot happen without his knowledge--#assumption) and the nodes are thus portrayed by connecting all the dots , here two of them being the leaders house and the madrasa.

The need for ground level analysis

Strategic Intelligence in military terms means the intelligence which goes into formulation of military policy and strategies. Operational intelligence on the other hand focuses on support to planning operations at the theater or regional level while Tactical intelligence is at the local level—intelligence that goes into driving operations locally.

Traditional intelligence doctrine does not take into account the asymmetric enemy which does not have an Order of Battle from the conventional enemy point of view—rather is dispersed, of loose cellular structure with all command identities unknown to cell members and is transnational..all in all near invisible with no military uniform that can identify him as in conventional battle , which does not resort to standard TTPs and other combat techniques, whose logistical, supplies and other support services are totally unlike the support arms of the conventional enemy and out of view, nearly invisible, hidden among sympathizers and communities resources. Thus if we consider COIN operations in a region, whether urban or jungle or hilly, the operational intelligence doctrine must be adaptive to include these factors. Further the intelligence, reconnaissance and surveillance platforms applied to conventional wartime and peacetime situations may not be as effective in situations involving, say COIN in an urban environment.

Hence we cannot just stay limited to traditional approaches to operational intelligence. We can adapt by say endeavoring to create new indigenous HUMINT sources, capturing indigenous insurgent technology conducting source operations by using sources from the local community by bridging the gap between them and us soldiers (developing close relationships, respecting their customs and abiding by it, being more of a civilian than a soldier by wearing civil attire and sharing tea/coffee with them, respect for their religion, etc all contributing to a conducive environment suitable for elicitation and oblique tactical prodding without raising any doubts) and conducting security reviews with such as the modern day IED in perspective..Information from all these being aligned with the intelligence requirements of the commander thus increasing the depth of his situational awareness.

The main goal of collection is to acquire data about the enemy's environment, resources, and activities. This is summarized as follows:

We need to know the current activity of the enemy, its objectives/goals, whether these goals are directed against us—the intent, whether it has the capabilities to achieve these goals and taken

for granted it succeeds in its attempts—that is it succeeds in achieving its intent , then what will be the consequences for us—the damage.

Intelligence here is crucial. We must determine the intent of the enemy. But like we are always striving to secure our installations, all related information systems and movements from enemy prying eyes so does the enemy who takes pain to cloak its behavioral indicators which might give out its intent. Now if there are no behavioral indicators, however we may suspect the enemy of possessing intent to cause harm, we are nowhere when it comes to determining it accurately. We need to go for deep intelligence collection and access a myriad of sources so that slowly the behavioral characteristics are discerned.

Here let's touch on Indicators and Warning concept. So vital to security. This is also known as Early Warning. If the enemy has intent it will decide on a course of action/actions—COA/s. We have to design a thorough collection system so that we can target the indicators (on a continual basis so as to confirm the enemy's COAs or negate our assessments of its COAs until finally we confirm accurately) and hence get an idea about the intent. And then lay down the potential COAs in parallel (parallel mind you) and after matching with the capabilities (yes, that too needs to be determined first) we choose the most probable COA of the enemy. The Early Warning system is more of a proactive-intelligence approach rather than a reactive-intelligence one.

For each intent they can take a course of action (or we zero down to a course of actions from a list of probable course of actions corresponding to the intent by considering more factors such as information gleaned from open sources, attack mode types or weapon types/delivery mode as per prevailing security hardening of target/security environment around/proximity of target etc) which we determine as most probable by considering factors like capability, behavior or other indicators. We can have a Most Likely Course of Action or in the extreme the Most Dangerous Course of Action. It all depends how successfully we ascertain their intent, capabilities, behavior and how far accurately we can infer their other characteristics and past criminal/terrorist/military offensive activity from past records/database **past threat assessments, past activity records, personality profiles, weapons/combat capability-strength, social networks (all these can be ascertained from open source, government records, criminal database, and detailed past activity reports**. For example a military unit, while assessing the threat can pull intelligence (of course on request and need to know basis) from higher headquarters, from adjacent units, from its own sources and from whatever ISR tools they have. Adjacent units or other units who share the same communication network or who is accessible by the unit can supply intelligence on the threats past behavior—say an engagement with the other unit. From that the unit can , within a good confidence level ,determine the enemy's tactics, techniques and procedures. Inputs like this can help in determining the probable course of actions. We can list out possible consequences for each course of action.

First the Intents, then ascertaining the Capabilities—not exactly ''then''...the collectors tasked by the CMO generally busy themselves with sourcing information on both and by pulling on

information from R&S teams.Therafter the Commander brainstorms with his staff the possible COAs by backwards iteration to the Intent/s and evaluating the COAs in the light of the Capabilities and also the possible consequences for the enemy/effects as battle damage or simply damage for us. A terrorist attack may more be directed at the Parliament House than a Mall because of the Symbolic and Political-Seat flavor).Again it can equally be likely that one enemy COA generates a crippling counterattack by our forces whereas another COA is less obvious and also causes less damage or less repercussion. The enemy too war games and may decide to forego the first COA and go for the second one. Another example could be the enemy's COA is simply intelligence activities directed against us with a timeframe to determine what they intend to determine, knowing very well that our CI teams will move in and take tentatively that time frame to expose their intent—hence their COA could be go on with the intelligence activities before the deadline—that is before they are exposed. There are several courses of actions, each in context of different scenarios. That is why it is immensely important to gain a perfect or near perfect situational understanding. Thus during this evaluation the Commander and Staff narrow down to the most possible Course of Action or the Most Dangerous Course of action for each Intent. Whatever every COA the enemy takes we must look for observable INDICATORS. This is the task of the Collection teams. Once these indicators are identified we look for patterns. Once we discern them we begin exploitation.

In other words, we need to judge the Intent of the adversary. Our intelligence collection teams should look for indicators, indicators which will tell us what he is doing today. Supported by more information about the capabilities of the adversary, , past threat assessments, past activity records , personality profiles , weapons/combat capability-strength, social networks (all these can be ascertained from open source, government records, criminal database, and detailed past activity reports).

We make an educated guess of the intent or a list of intents with confidence level/s and then list out the corresponding course of actions with possible consequences for each course of action. Continuing the iteration further we select the most likely course of action and the most dangerous course of action by studying the consequences along with the capabilities and intents.

The following grossly sums up the steps in the intelligence cycle.

1. Develop intelligence requirements.

2. Collect information to answer intelligence requirements.

3. Triage information for accuracy and consistency, analyze collected information, deconflict inconsistent information (if necessary), and identify other intelligence requirements (re-task collection, if necessary).

4. Compile analyzed information (timely, accurate, specific, and predictive!), and produce a finished intelligence product for dissemination and community consumption.

This all goes back to collection. What are the goals of the adversary? What's he trying to accomplish; what's his intent? What is the Order of Battle of the enemy? In other words what are the strengths, dispositions and capabilities of the enemy? What is the inventory and type of their equipment/weapons? How will the terrain affect enemy's movements, possible courses of actions (this applies to us also),what are the possible concealment areas offered by high ground or foliage, how does the terrain afford ambush points and where they can possibly be, how does the current and future weather predictions act as enabler or otherwise for the enemy and us, what is the present enemy situation , if the enemy is an asymmetrical one like the terrorist/insurgent then does it have the capability to attack hard targets, what was the modus operandi in the past of the asymmetrical enemy, target history and who were/are its leaders/sympathizers, what were the safe houses then and possible locations at present, what ideology the terrorist group pursues and what are its aims as demonstrated by its propaganda or by website declarations and so on. ***This will allow us to identify indicators. We identify indicators, then patterns, and then we exploit them.***

Tracking adversary capabilities is a continual process, and should be updated per changing conditions in their strength, disposition, equipment, or tactics, techniques and procedures (TTPs).

Requirements Determination –The Collectors

To properly collect information during war or any situation involving ground troops and the enemy, be it a tactical operation or stability operation we need individuals who can interrogate or EPWs or detainees in an efficient manner without invoking unnecessary delays .

To this end we need persons with good interrogation skills, ability to conduct tactical questioning and good debriefing skills. Soldiers on the ground need to be trained in HUMINT capabilities, apart from HUMINT specialists, so that when the soldier encounters the EPW right at the front or in areas other than the rear, he can quickly interrogate and extract HUMINT/CI relevant information and then pass on the prisoner to the interrogation facility. If the soldiers manage to

extract information this way, it could very well be that the said information can be of immediate tactical use to the unit the soldier belongs. The chances of detaining an individual with no information or intelligence of target value are also lessened considerably. On the other hand involving soldiers this way helps the commander and upper echelons get a first hand good situation assessment.

Besides this we need trained HUMINT specialists to act as enablers for the commander while assessing the situation. They will conduct source operations to throw light on the enemy order of battle, his capabilities, plans and intentions. The collection manager with all the inputs from the HUMINT specialists can then assist the Commander with updating his intelligence requirements and with the capabilities and intent of the enemy in perspective now, he can devise appropriate COAs.

As for the intelligence component CI we need to realize the full import of the latter. Thus we need CI specialists/soldiers with the skill to identify, detect, counter, neutralize or exploit the enemy's intelligence approaches to gain information about our plans, capabilities and other factors. The CI soldier must be well versed in polygraph and technical countermeasures as there can be cases of treason and subversion and he will have to identify, detect such individuals and also establish their complicity in the crime and report to the executive. Foreign language ability will be an asset.CI soldiers need to exploit documents seized and these may be in a foreign language.CI teams can be augmented with an interpreter in case the soldiers lack the ability to converse in a foreign language.

Finally we need soldiers/specialists trained to coordinate collection activities, deconflict and synchronize all HUMINT/CI activities and interact effectively with higher and lower echelons.

ORGANIZATION OF PROPOSED ORGANIC INT UNIT FOR PARAMILITARY BN FIGHTING INSURGENCY

Command includes the authority and responsibility for effectively using resources, planning for and employment of forces, and ensuring that forces accomplish assigned missions. Leaders and staffs exercise control to facilitate mission accomplishment.

We can have the following organizational structure:

The HUMINT Analysis Cell (HAC)

HUMINT Operations Cell (HOC)

Operations Support Cell

Counterintelligence Coordinating Authority
HUMINT Teams

HUMINT TEAM HQ - Analysis & Control Element: An Intelligence mission management and analytical hub at the division, corps, or theater level, where intelligence is gathered from the individual intelligence disciplines and fused together to form a composite intelligence picture. Gaps in intelligence are identified and tasked out to the respective collection assets.

ACT - Analysis Control Team: An intelligence cell which aids tactical combat brigades or battalions in managing assigned or attached intelligence assets and conducting analysis.

OMT - Operational Management Team: Manned with a mix of CI/HUMINT soldiers led by a CW2/CW3, the OMT is designed to manage two to three subordinate CI/HUMINT Operational Teams (OT). The OMT is a self-contained operational and technical control and analysis element. **The OMT is capable of plugging into an ACT, ACE, Rear Area Operations Center (RAOC) or any element which has a CI/HUMINT requirement.**

HOT – HUMINT Operational Team: Manned with a mix of CI/HUMINT soldiers led by a WO1/CW2, the OT performs CI/HUMINT operations, investigations, and collection functions.

TET - Tactical Exploitation Team: The TET is subordinate to the Corps MI Brigade and contains the Corps CI, IPW, and LRS assets.

The HUMINT Analysis Cell (HAC)

HUMINT reports and other operational feeds need to be worked upon, processed, and derivations made. Cross cueing with reports from other sensors sometimes becomes necessary.HUMINT validates IMINT, SIGINT.What we need is a cell where all these feeds are fused together, processed and timely actionable intelligence derived. Extrapolation is also done to impact operational and strategic considerations with the available intelligence products plugging into the overall intelligence system. The HUMINT analysis cell also indicates gaps in reporting.

The HAC:

Produces HUMINT reports and feeds for intelligence summaries. Conducts dissemination.

Maintains database of all HUMINT activities in the AO and this database is directly accessible to all HUMINT teams and lends very good support to their collection operations.

HAC plugs in ACE so as to use analysis tools for immediate and long term analysis and collection plans. It analyses the trends and patterns discerned after collection or during collection. Analyses source reliability and credibility by various comparative tools and assists the collector to know his sources better and assign tasks accordingly or stop all source-handler operations with sources of negative attributes.

HAC helps in compiling target folders. Now future collection efforts can be affected based on the information in these target folders. The target folders are updated time to time and a repository maintained.

HAC supports CI entities by supplying information of CI interest and provides feeds to CICA

- Provides collection requirements input to the HOC.
- Supports RM through the development of HUMINT SIRs based on command PIRs.
- Answers HUMINT-related RFIs.

HUMINT Operations Cell (HOC)

Coordination and synchronization of all HUMINT activities is of utmost importance.Proper technical control and deconfliction among adjacent and higher/lower HUMINT elements is the job of the Operations cell.The HUMINT Operations Cell HOC.The HOC keeps a track of all activities conducted by all HUMINT and operational teams(which are a mix of CI and HUMINT operators) and coordinates them. The HOC in the *2X coordinates and synchronizes all HUMINT activities in the AOIR. The HOC-

HUMINT TEAM STRUCTURE

Operational Management Team

6-56. The OMT is manned by 3-4 persons and provide technical control, operation coverage and guidance, collection and operational advice and focus to 2-4 HUMINT teams who are engaged in the actual collection and other HUMINT activities. The OMT can have an analysis element (to help in quick dissemination of actionable intelligence) to assist in boot-level analysis and mission analysis. It reports teams equipment status and other variables which may affect the HUMINT teams capability to the HOC and unit headquarters. It works in close tandem with the ACT to develop current threat assessments and answer the commander’s intelligence requirements· Provide the collection and operational focus for HUMINT teams.

Integrates the HUMINT teams directly into the commander's ISR planning. Keeps the commander abreast of all activities, capabilities and limitations of the deployed HUMINT teams.

HUMINT Team

The HUMINT team consists of 4-5 persons who carry out the actual HUMINT functions and are trained in the entire spectrum of the latter, and they may be deployed to execute mission-focused activities of interrogation, debriefing, contact operations, tactical questioning or DOCEX.

The HUMINT-CI mix (Tactical HUMINT team) functions:

CI/HUMINT Preparation of Battlefield:

CI/HUMINT team will study all environmental factors and the effect they will have on both the enemy and our forces.

Attention areas:

Threat profile including Intent,OB,Dispositions,Strength,TOE, Demographics,population,politics,culture,language,ethnicity,history,religion,military,terrorism,insurgency,information structures, communication lines, centers of gravity and other criminal groups who support enemy/sympathizers from local community intentions/attitudes.

Enemy's Composition, Disposition, Strength (often mnemonic zed with):

SALUTE: Size, Activity, Location, Unit, Time, Equipment

Exercise:

I as the Commander have a Goal. To determine the Threat capability of the enemy. To this end I define the mission as explicitly as possible. Thereafter I set down the PIRs. At the same time the HUMINT resources I can spare are allocated tasks to collect information after my planning team in concert with the collection manager sets up cells each catering to certain IRs broken further into several Sirs. The teams of HUMINT and TACHUMINT are guided, controlled and overseen by the OMT, HAC….

Goals: We need to determine the intent of the enemy (threat) ,as formulated by the command (top hierarchy whose identity we need to determine),its strength, disposition and capabilities and all the possible courses of action, the most likely course of action and the most dangerous course of action.

PIRs: What are the intentions of the enemy and is it capable of carrying out the threat?

TASK: Each team derived from each cell will consider all factors and generate the intelligence requirements. They will then task themselves with identifying all indicators that support or deny these intelligence requirements

Identify the threat's likely objectives/desired end state.
Identify the full set of COAs available to the threat.
Develop each COA.
Evaluate each COA.
Prioritize each COA.
Identify threats to aviation operations for each COA (Aviation-specific).
Identify initial collection requirements.
Identify initial production requirements.
Identify initial dissemination requirements.

A. We can create a basic intelligence team structure with the GOALS:

1. To identify the enemy top-tier officials
2. The enemy intent (current tactical goals and strategic goals)
3. The strength, disposition, capabilities assets, and organization structure of the enemy.
4. Organizations TO&E
5. The most likely COA and the most dangerous COA.

B. From the above we identify our primary intelligence requirement/s:

The immediate threat posed by the enemy. What are the goals of the adversary? What's he trying to accomplish; what's his intent? Answer what he's doing today in order to answer what he's going to do tomorrow and beyond.

C. Next we create teams, say 2-3 manned teams, each team assigned a separate task of collection. The team leader should exhort his members that given the intelligence requirement by HQ they should strive to generate further IR based on the information available and during collection as new information may require further probing and exploration. Members and team leader should be proactive. Intelligence too is both reactive and proactive. An indicator associated with an IR propels the agent to look for corroborating information--that's reactive. Sometimes we are totally unaware of the unknown. Well the intelligence agent can have an informant/source network in place which constantly looks for say enemy movements or any

change in enemy positions—which on first sight can be a normal movement/displacement but on further probing reveals an offensive intent. To this end the intelligence agent needs to have a proactive mindset, always curious, probing and exploratory.

We also set up covert or overt civilian collection units whose members are either having access to physical addresses frequented or inhabited by the enemy or are geo-located in close proximity to the latter.

Our teams are exhorted to resort to open intelligence frequently OSINT such as any news/enemy propaganda/private and government discussion boards, analyses/TV panel discussions on current situations with reference to the disturbing elements posted on the web, in dailies, or aired on radio / TV programmes.It should be borne in mind that globally 90% useful intelligence is collected from OSINT sources and the remaining from ISR platforms.

Our teams can be based on the following factors – ATTENTION AREAS:

- Organization,Composition,Disposition,Strength (the command structure and organisation of headquarters and subunits, geographical locations of unit headquarters and subunits, Strength expressed in units and weight of fire delivered by its weapon systems)
- Leadership
- Intent
- Weaponry and Equipments
- Capabilities / Combat effectiveness
    - TTPs—historical in the concerned area of operations and area of interest.(Tactics used by the enemy unit and Miscellaneous data related to specific task, mission or operations…this will help in determining enemys most likely course of action. Unit history used to judge expected performance based on its past performance)

- Threat ranking-by violence or activity
- Enemy propaganda
- Recent incidents of violence irrespective of sporadic or concerted nature
- Local community and political support
- Other friendly groups / criminal gangs sympathetic to enemy causes or having same ideology/political goals
- Logistics

Keeping the above factors in perspective we can create cells comprising of HUMINT collectors (and also admixture of HUMINT/CI , TACHUMINT—when information of CI Interest is emerges when the HUMINT collector is conducting questioning , he will transfer the source to the CI team).These cells may be:

- Leadership Cell
- Enemy units cell
- Strategic Cell
- Threat Cell
- TO&E Cell

Each team cell will generate its intelligence requirements. These requirements are all predicated by the Commanders PIRs.SIRs or sets of SIRs corresponding to each IR are developed, keeping in view the indicators.Therafter tasking begins.

The current teams are C2, Strategic, Lower HQs and Units, TO&E AND THREATS.

C2 Cell – The enemy organization leadership formulates the strategy and hence the individual leadership personalities, their affiliations, intent, movements, social contacts etc should be gauged accurately by identifying the indicators so as to defeat their ongoing or future deliberate operations. The hierarchy should be determined which will give us an idea of the functions and span of control of each level. Thus the C2 cell will focus on the command and control of the organization.

Strategic Cell: Decides on the overall strategy. Is composed of the Command staff, planning, logistics, operations and intelligence/CI advisors.

Lower HQs and Units cell – The organizations middle and lower level management is composed of lower HQs/Section HQs and units. The capabilities of these should be determined and it should be assessed properly as to which deptt or unit has a significant part in the current operations against our forces and thus we can assign a priority ranking. This ranking can be based on the threat potential or activity predicated by the overall intent of the organization which has prompted it to conduct current operations. That is to say those HQs and units should be prioritized as per their threat capabilities and activities which have a direct bearing in the offensive operations.. Triage all these HQs and units and feed the report to the TO&E cell.

TO&E cell – The TO&E cell will evaluate the report submitted by the Chapter cell. It will evaluate the strength, assets and activities and draft a table of organization and equipment.

Threat cell: The task of this cell is to identify all the possible courses of action to be undertaken by the enemy and distill them to infer the most likely and most dangerous course/s of actions. The threat cell will consider all the inputs from the other cells. In addition it will undertake an intelligence preparation of the battledfield.It will study the past violent behavior of the enemy,

take cognizance of its intent/s, capabilities, dispositions, strengths, affiliations with other support elements such as criminal enterprises, terrorists and create intelligence requirements, prioritized which will lead to tasking of its operatives to identify the indicators supporting or denying these threat activities.

COLLECTION SUMMARY

Assessment of threat capabilities, operations and, current and expected threat actions across the battle space to provide the commander with an assessment for the development and execution of countermeasures.

Recommending countermeasures after assessment of threat capabilities, operations, expected courses of actions, most likely COA and most dangerous COA.

Threat intent

Identify Threat leadership. Key commanders. Key lieutenants and area commanders

Identify threat C2 nodes

Identify threat logistic routes

Identify threat social reach, network, and contacts

Identify threat affiliates in other criminal networks, enterprises

Identify threat sympathizers in own area of control

Identify political/administrative figures that support threat ideology

Threat attack /defense operations location parameters.

Gauge potential attack/defense methods of threat.

Recommend C2 setup to thwart threat attack.

Estimate with reasonable accuracy the expected time of attack.

Possible locations of Threat listening post/observation posts

Determine possible escape routes of threat forces after an attack or defense scenario

Possible enemy IED techniques, infiltration routes, emplacement

Gauge IED detonation methods/means

Gauge IED timings

Possible routes for IED ex-filtration

Staging areas

Safe houses

Weapons and ammunitions storage locations

Production facilities for IED and other ammunitions/explosives.

Find out what supplementary operations threat may resort to

Recommending countermeasures to threat IED

Recommending countermeasures to threat ISR/EW

Determining threat indirect fire parameters, key indirect fire

WARNING

(a) **Warning**. **Once actionable intelligence is obtained warning or predictions is disseminated in a timely,unambiguous,specific and accurate manner.Warning is an acknowledgement of the existence ofd a threat and subsequent disseminating.**

Warning is of two types:

- Defensive warn
- Enemy warn

In defensive warn after receiving actionable intelligence about the adversary's possible attack the installations security is beefed up by incorporating protective measures. The warning may be digital/aural/physical or virtual.

In enemy warn the enemy is communicated the fact through non-lethal measures such as interrogation or challenging an enemy unit/capability that in case of persistent or continued enemy action our course of action/s can take on an increasingly lethal nature with the intent to prevent the enemy from taking further hostile actions and also inflict heavy damages. Thus enemy warn is a method to deter the enemy from carrying out its intent if it hasn't done so yet or to stop the enemy in its tracks.

It is very important that warning should be unambiguous, accurate and timely/specific. In addition to this it should be actionable. Warning can be graduated; meaning the level

of warning may assume increasing proportions in keeping with the feedback about the enemy which may indicate that it has ceased its operations/.activities temporarily but is conducting discreet operations/increased intelligence activity masked in the cloak of acceptance of our warning and cessation of open hostilities.

WARNING SYSTEM:

The warning system must have the following features:

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, and 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

(b) 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.

METHODOLOGY OF INTELLIGENCE COLLECTION:

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

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

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

The six steps in the CM process are:

- Develop Requirements,
- Develop a Collection Plan,
- Task/Request Collection,
- Disseminate,
- Evaluate Reporting,
- Update Collection Planning.

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

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

- Commanders Priority Intelligence Requirements
- Low Priority Intelligence Requirements
- Requests from subordinate units,
- Taskings from higher HQ's
- Intelligence requirements for targeting purposes

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

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

COLLECTION FORMAT

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

In the latter case the following steps are followed:

- List the PIRs and IRs, prioritize them and enumerate them using control numbers and alphabets. This helps in prioritization.
- Now ascertain the indicators
- Determine potential indicators-prioritize those that will answer the PIR and IR.
- Delete all indicators that do not answer the intelligence requirements.
- Develop specific intelligence requirements. These are the requirements as stated by the commander, prioritized and general, broken down into manageable specific requirements. A PIR may have several specific intelligence requirements.
- Analyze these SIRs and the target characteristics keeping all the indicators in perspective.

- Finally prioritize the SIRs and determine the suitable collection discipline/platform/agency keeping its capabilities, limitations, backlog of collection tasking allotted to it and whether adjacent units, lower units are also using it.
- Prepare the tasking list by creating a prioritized SIR list and deploy the collectors.

Indicator analysis is the basis for recommendations to the commander for a specific COA.

Note:

1. Intelligence should be timely, accurate, predictive and specific. The last term is very important especially in the case when actionable intelligence is needed. The HUMINT agent reports:

- Observed movement of Bodo insurgents in NAI 6.
- Observed that they are moving south towards the rice fields near the Tarmung village

Now these two reports are timely as they are happening right now, predictive as we know they are moving south towards the rice fields near an identified village. But what about specificity. What is the strength of the insurgents in terms of manpower? How many of them? Any idea how heavily are they armed and what weapons are they carrying? Do they possess mortars, bazookas, rocket launchers (shoulder mounted)? Where are they exactly in named area of interest 6? Whenever you report keeping the factors Size, Activity, Location and Time in perspective, you need to be as specific as possible. That way we can not only gauge their exact intentions and courses of actions but also formulate our course of action, as we can now pin-point them.

Enemy Capabilities and Limitations can be mnemonic zed with **DRAW-D, Defense, Reinforce, Attack, Withdraw and Delay.** The Order of Battle and Table of Organization and Equipment (ORBAT and TO&E) are two areas intelligence must dwell upon throroughly.The ORBAT refers to the enemy organizations disposition, capabilities assets and composition whereas TO&E refers to its organization table of units and associated equipment. Thus the Commander is made aware with this strength, disposition, organizational and capabilities brief of the enemy.

Tasking is meted out considering:

Type of collection platform to be used. Here it's HUMINT

Availability of HUMINT resources. It could well be resources are very limited. Maybe time is of essence. It could well be that actionable intelligence is required fast and there is no room to send the collected information up the chain for collation, processing and dissemination to targeting platforms by the end-users—here the Commander. This time constraint may mean we have the analytical element right at boot-level, who will be a part of the collection team. This will cut down on the time involved in the intelligence cycle from collection to dissemination. Moreover

availability of HUMINT resources also means the Commander has other priorities with other tactical missions or maybe a part of the HUMINT resources are away accompanying patrols to get intelligence from neighborhoods, civilians etc.So availability of resources is a criteria to be taken into account.

COMMAND AND CONTROL

HUMINT COMMAND AND CONTROL

Commanders that conduct HUMINT operations take responsibility for:

- ✓ Constituting task organizations
- ✓ Assigning missions
- ✓ Execution of the mission
- ✓ Mission accomplishment
- ✓ Designating the AO for each mission tasking.
- ✓ Commanders must ensure mission accomplishment by optimally allocating resources and logistics to support HUMINT operations,keeping in mind the constraints and time.The Commander should make adequate arrangements of training of his MI unit personnel.There should also be cross training of HUMINT operators and HUMINT applications personnel.Each should know the others method of operation.Thus he can ensure the operational readiness of his personnel.The Commander analyses higher headquarters intelligence requirement,requests for information from adjacent and subordinate units,tasks his organization,states the mission,tasks the HUMINT collectors,executes the mission,accomplishes it and conducts a post operation review,manages any discrepancies or gaps in intelligence(maybe again tasking his men).He is accountable to and responsible for all HUMINT activities and should see that they confirm to doctrinal guidelines.At this juncture he should fully liaise with the technical control team and OMT. He issues mission orders to subordinate unit commanders , being as deatailed as possible and giving as much time as can be allowed.

Commanders must:

- ✓ Must understand and know the enemy, his organization, his ISR capability, his counter-ISR capabilities, his threat platforms, and the terrain over which it exercises control and how the terrain can be an enabler for his HUMINT/C-HUMINT operations.
- ✓ As regarding his own HUMINT units he should understand the constraints, technical and operational, under which they function
- ✓ Should ensure synchronization of operations with intelligence

- ✓ Should ensure the best training of all personnel in his units
- ✓ Optimum reconnaissance and surveillance in close co-ordination with higher HQ, adjacent units, subordinate units and staff is very important--he should implement this.
- ✓ Should keep higher HQ informed of manpower, equipment, logistical and operational updates, any shortcomings, requirements or any enhancements required. Advises higher HQ of capabilities and limitations of his HUMINT assets.
- ✓ Should continually supervise each and every operation, create a feedback system and use the feeds to ensure high quality and technical control of both the operations and HUMINT products.
- ✓ Ensures personnel are working within legal, regulatory, and policy guidelines.

Technical control is not a C2 function but intelligence operations do require it to be effectively executed.HUMINT, SIGINT and CI operations often require technical guidance and control. Multidisciplinary intelligence operations require technical control so as to adhere to existing policies/regulations and Tactics, techniques and procedures (TTPs).Technical expertise is resorted to by the Commander while directing operations. The 4 phases of the units collection activities, viz..Plan, prepare, execute and assess are detailed and designed with the help of technical experts Technical control includes, but is not limited to–

- Defining, managing, or guiding the employment of specific ISR assets.
- Identifying critical technical collection criteria such as technical indicators.
- Recommending collection techniques, procedures, or assets.
- Conducting operational reviews.
- Conducting operational coordination.
- Conducting specialized training for specific MI personnel or units.

INTELLIGENCE CAPABILITY WITH CI

C2

We must have a command and control structure to properly utilize the intelligence resources and operations. The commander can then exercise control over the subordinate units and operations. He can establish the degree of control and authority of subordinate commands. Relationships among the subordinate units and adjacent units can be smoothly managed if a clean command and support relationship exists. Thus the subordinate units and supporting units can have well defined responsibilities and authorizations. Thus the commander designates command and support relationships within his span of authority and all these subordinate commands and support units go hand in hand to decide on schemes of maneuver and operations progress. Thus

all the forces under the parent commands tactical control receive the best guidance towards mission success. Accountability will also be enforced properly. In intelligence operations technical control is of importance. Technical control is strictly not a command and control function but it is a control function ensuring that adherence to existing policies,regulations.TTPs are maintained and provides for technical control of MI operations. Establishing clean command and support relationships is fundamental in organizing for all operations. These relationships can achieve clear responsibilities and authorities among subordinate and supporting units.

We must have a command and control setup which will incorporate management, analysis and control of all-source intelligence, and technical control of the operations of the respective intelligence disciplines. Thus we will have a HQ with 2 section HQ's under its control. Communications would come directly under HQ purview. One section HQ will look after the All-source production team, collection management team, target nomination team, dissemination team and operational management team. The other section HQ will be the technical control element looking after the HUMINT, CI, SIGINT and IMINT Teams.

The All-source production team will have a HUMINT platoon, a CI platoon or a combination of the two—a Tactical HUMINT platoon and if assets are available an IMINT team. The Tactical HUMINT Platoon can have a HQ designated authority, a HUMINT Control team, three HUMINT Teams and one CI Team. The CI team may be further divided into 2 teams composed of 2 operatives each. Mission requirements define size and composition which can vary from the stated composition. The CI team will conduct CI Investigations, assessments and C-HUMINT ops but may not engage in C-SIGINT or C-IMINT as it hasn't any organic capability.

Now the tasking is assigned to each team. That is to say the IR for each team.

TASKING EXERCISE

Requirements are primary and secondary.

Primary requirements. For instance, our PIRs and IRs might look something like this:

PIR 1: What threats exist in our AO?

PIR 2: What threat activities occur in our AO?

PIR 3: What targets are the threats likely to attack?

IR 1: Define the threat operational tempo.

IR 2: What is the strength and disposition of the insurgent group?

IR 3: Identify the leadership of the insurgent group.

IR 4: Identify the facilitation/logistical networks of the insurgent group.

IR 5: What locations are associated with the insurgent group?

So on and so forth. These are our requirements that we must answer through collection, whether it be Human Intelligence (HUMINT – including surveillance and reconnaissance) or Open Source Intelligence (OSINT), or whatever other means are available.

Some guidelines for TACTICAL QUESTIONING for the created unit personnel:

***Tactical questioning.**

Generally soldiers conduct two types of collection--passive and active. On the whole soldiers should practice the former generally when they are not asked to look for prioritized information..which are generally the domain of trained collectors, say HUMINT specialists(active collection).Passive collection should be practiced by each and every soldier if time allows or opportunity presents itself--say a casual query to a local , or elicitation or during patrolling when you project a friendly attitude in the local community and during conversation you glean information of tactical value.

Active collection:-During tactical operations in a COIN environment for example, actionable intelligence and follow-on missions to kill/capture is depend a great deal on the soldier-on-the-ground--the tactical questioning ability of the latter. In such operations, say after a fire-fight, once the operation is over and the prisoners taken and the area secured, the local populace is rounded up and questioned for further leads or to identify any insurgent in hiding among the populace by observing his demeanor on questioning. In yet another scenario, say post-IED blast, again the locals can be questioned. Clues may surface, say there was this stranger who had visited the area just prior to the blast, wearing such and such clothes and travelling on a motorcycle with license plate number of a different city. Maybe that person is still in the village. He is picked up, interrogated and a wealth of information extracted which could be valuable actionable intelligence, driving further operations. In other instances of tactical questioning, routine patrolling to villages or areas of interest near the military area can yield good intelligence after contact is established with the local population. They might offer information on the daily activities of suspects and their possible whereabouts.

The intelligence unit which was just set up has as its main control center the ACE. The ACE hands out the tasks to the various specialized personnel to conduct active collection operations--tactical querstioning,interrogation,debriefing,interviewing and DOCEX.Specialised personnel are needed because the average soldier will not be able to probe with specially designed questions or have a technical mindset characteristic of HUMINT/CI agents.

Some steps for TQ:

Plan in advance. For that you need to know the intelligence requirements as laid down by the collection manager or ACE. The scenario can be ascertaining certain facts of the enemy from a local: What did he exactly see? Whom did he see? Does he know him or is he a stranger? What was he wearing? Anything out of the ordinary in his attire? Was it uniform-like? Was he dressed in expensive outfit? Did it look like his clothes were concealing weapons? Maybe his jacket was too heavy--bomb strapped inside to his body? Which way did he go? Other men were there with him? This way you should probe him--always open-ended questions instead of yes/no questions.

Note a difference here. We are simply questioning him directly instead of first planning an approach like the interrogator. In certain situations time is of essence. We need actionable intelligence straightaway. As the insurgent group needs to be dealt with immediately and he/they are nearby with intent to mount an attack on our forces in the immediate future. And they sometimes take sanctuary in this village by mixing with the crowd or maybe they this village is a permanent node in their passage route to their safe havens. Tactical questioning is a **direct approach**.

We can set templates for tactical questioning. That is a typical list of questions fitting a typical scenario. So we brainstorm several scenarios beforehand and have a good list of questions. Brainstorming beforehand means much before any imminent operation, not that we have need for actionable intelligence in 24 hours, and we set down to brainstorm questions. The templates are the task of the research people at the ACE.

Going by ACE requirements--the intelligence requirements--can prove to be a very good tactical questioning operation. This is where technical control becomes important. In tactical questioning one should adhere to ACE requirements and question directly, open-endedly.The ACE might be needing a composition, strength and disposition report of the insurgents. Who do you think was the leader of that suspicious group you saw in so and so place? How many of them were there? There were women; we have information. Now how many women were there with them? Were they armed? Do you have any idea about the maker of weapons? Fine you don't know how did the weapons look like? Rifle-type or is it like this I am carrying? Or is it like the one you see with the local police? Do you have any idea where they can get accommodation? Anyone having a place of stay here who usually gives it out only to people from outside your area?

The ACE might be looking for possible targets of attack by the insurgents. This is a way of predicting future attacks by analyzing soft targets. Well do you think the religious structure will

be bombed by the insurgent/terrorist? If so, why? You are the better judge, aren't there any other more important possible targets, the bombing of which can cause good loss in life and more important than that cause widespread panic and media attention? And so on.

During the course of tactical questioning often the collector lands up with sources that have good placement and access to the required information. The collector refers his data to the ACE who register his name and bio in the source database and also update the target folder with this particular source giving information on a particular target.

More on TQ in Appendix.

NOTE ON SCREENING – A VERY IMPORTANT PREREQUISITE DURING LOW LEVEL SOURCE OPERATIONS:

Screening

The HUMINT assets deployed to conduct source operations are always exceeded by the number of available prospective sources and documents. Hence screening is of utmost importance and an absolute necessity to determine the right sources who will offer the right information and in another scenario are not enemy agents themselves. Efficient usage of limited HUMINT resources thus becomes feasible.

HUMAN SOURCE SCREENING

Screening is of two types. Human source screening and document screening. In Human source screening it is determined whether the source truly has prioritized information needed by the Commander, meaning whether he does have the required placement and access to the information. A predetermined source-profile is often laid down after ascertaining the intelligence requirements. Screening attempts to locate sources who match this source-profile. Screening also determines whether he has any information useful to any other agency , such as the CI unit and hence is referred to the unit by the HUMINT operative (this is the case in tactical HUMINT units and mobile interrogation teams , which besides being composed of HUMINT assets have a 2-3 CI member team included).It should be remembered that already HUMINT resources are insufficient , and hence a balance should be maintained between employing them for screening and those that conduct interrogation, debriefing and other HUMINT operations. **Screening is an integral part to all HUMINT collection operations. While questioning an individual source, a HUMINT collector may switch between screening (finding out general source areas of knowledge) to interrogation, debriefing, or elicitation (finding out**

detailed information about a specific topic). Screening is not an information collection technique, it is the evaluation of prospective HUMINT sources but it is very necessary for the collection operations to succeed as it targets those sources that can be exploited best by the HUMNINT agents to extract the prioritized information requirements as per the HUMINT mission or higher headquarters needs. Hence screening should be conducted by personnel who are totally knowledgeable of all HUMINT collection operations , the intelligence requirements as laid down by the collection manager and who are sufficiently matured and experienced to study the source and make well reasoned judgment based on limited information.Yes,to optimize HUMINT assets deployment collection (interrogation,debriefing,elicitation) can be integrated with the screening process but then this slows down the overall tempo of the HUMINT mission.

The purpose of screening is to

- Identify those select individuals among the target audience who have information of potential value and who are willing or can be persuaded to cooperate.

  Identify individuals who match certain criteria that indicate them as being potential subjects for source operations or matching the profile for collection by special interest groups such as TECHINT or CI.

During screening certain preliminary criteria are kept into consideration which is indicators of a source possessing potential information of use to the Commander. These criteria include rank, position , gender , appearance and location. Criteria such as occupation may require questioning. Others may be determined simply by observation.

Screening is of prime importance, in fact the most difficult HUMINT task. Only if screening is done properly can HUMINT assets deployed be put to the most efficient use, otherwise time, effort and HUMINT expertise wasted and tactical or mission objectives not attained.HUMINT assets are frequently very few in number compared to the enormous quantity of detainees during an ongoing operation. There can be no room for wastage of these assets or working on wrong/useless information extracted from a poorly screened source. Screening places in the hands of the HUMINT operatives the right sources with the right placement and access to information required. If screening is done incorrectly or without focus , say without the exact collection requirements in mind then what results is a mix of sources with little or absolutely no information. As such screening is of prime importance and requires very trained personnel. They should have long experience, should be aware of local cultures and norms, should be able to understand the psyche of the source, have good assimilation, analytical and questioning skills language capability, and the ability to understand perfectly collection requirements, break them down into all possible indicators and look for source-profiles who can give information relating

to these indicators. The screener should also be able to examine the source carefully and determine if he has any information of use to other intelligence disciplines.

One very important point to be noted here is that screening may have to be executed in a very short span of time, say at the front or near the front during combat operations and where the detained personnel need to be examined very fast for actionable intelligence. Before the HUMINT/CI operatives do that the screener should rapidly segregate and process the detainees. Thus he should be highly skilled in screening. Yes screening and other HUMINT operations like interrogation can be switched to and fro on the same detained personnel group to save time.

SCREENING REQUIREMENTS

As mentioned before screening should be driven by collection requirements. Just like any other HUMINT operation is driven by intelligence requirements. The collection requirements should be very clearly understood by the screener. They should not be vague, but explicitly clear. If not then the screener must extend his faculties and imagination to create indicators from these vague requirements (IR, SIR).Screening is relating the knowledgibility brief of the source with the information requirements and ascertaining how close does it match the latter.

Usually the intelligence officer breaks down the PIRs into SIRs and looks for indicators. If not done yet the screener should be adept in determining the indicators corresponding to the SIRs and these indicators must reflect the anticipated source-profile to identify EPWs and detainees who might possess information pertinent to these indicators. The source must be presented with an enquiry which should be more elaborate or else good selection of sources isn't possible as the HUMINT operative cannot gauge the knowledge of the source with regard to the intelligence requirement at hand. For example asking the source ''Are you aware of any camps of the insurgents in your area'' won't be of much help—its vague. The source might not know anything at all of the existence of insurgent camps in his area. But he might very well know that certain elements of dubious nature carrying arms frequently go south towards the remote jungle area, strangers visit his village occasionally and rent homes for few days etc.Hence the HUMINT operative must frame his questions (SIRs).These indicators must relate to source personality, characteristics and types. For example, a refugee probably will not know if the threat intends to defend a particular ridgeline. However, he might know whether or not there are threat forces on the ridge, if an improvised explosive device (lED) is being employed on a route, if they are digging in, or if engineer type equipment is in the area.

UNIT SUPPORT TO HUMINT COLLECTION

Small units contribute to HUMINT collection through a number of different ways.

Every soldier is a Sensor—this statement is a major transformation in Intelligence Doctrine. It should be strongly emphasized that dedicating/deploying only multidisciplinary intelligence collection assets is NOT enough. The soldier on the ground, who is in direct contact with the local environment, be it at times of small scale operations, patrolling missions, handling EPWs/detainees or captured documents – HE IS THE EYES AND EARS OF THE COMMANDER.

- ✓ Hence a culture of intelligence collection, or in other words a natural tendency to probe and collect information—should be inculcated in each and every soldier, irrespective of trade or speciality.This is Tactical Questioning which is guided by the units SOP, ROE, and the order for that mission. Tactical questioning aids in proper visualization of the existing situation (Situational Understanding of the Commander) by enabling the soldier to conduct **expedient enquiries** in order to extract critical mission-specific information of ***immediate tactical value.***
  Soldiers can conduct TQ when they are:
- ✓ Manning a check post/roadblock
- ✓ Executing traditional offensive/defensive operations
- ✓ Handling detainees/EPWs during the very initial stages of apprehending them
- ✓ Handling captured documents
- ✓ Occupying an OP
- ✓ On a patrolling mission
- ✓ In conversation with the local populace after an operation and securing the area
- ✓ Conducting questioning as MP personnel
- ✓ Passing through an area in a convoy
- ✓ Involved in any operation whatsoever where they get the opportunity to observe and report on environmental factors – factors pertaining to the mission/Area of operations

ISR Operations

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

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

- Reporting immediately any information the soldier considers of critical tactical value. The Soldier may resort to his commonsense/experience or any predetermined criteria to arrive at his judgment
- Normal reporting
- Information during normal debriefing sessions by the intelligence officer.
- Follow-up reporting, after debriefing by the intelligence officer is over.

Collecting HUMINT

The screening of human sources is the first step of the HUMINT collection. This process includes conducting interviews that would be cross-indexed as well as recorded on an essential basis. Small bits of information can state different meaning in the HUMINT context which is why it is required that the interview should be planned carefully and intelligence collection discipline is observed. This planning is also essential when the interrogator is not part of the same culture of the respondent and does not speak the same language.

Multidimensional Reconnaissance and the HUMINT Platoon
UNIT EXERCISE

Multidimensional reconnaissance is a field which the HUMINTR platoon should be well versed in. The MI company platoon belonging to the Brigade primarily conducts source operations. The OMT sends all information collected by the tactical HUMINT teams (comprising majority HUMINT and one or two CI operatives) to the STAFF INT OFFICER for integration and deconfliction with outside sources.

There are 2 configurations of operation of the TACHUMINT teams.GS and DS. In the GS mode the teams come directly under the control of the Brigade STAFF INT OFFICER and the OMT of the HUMINT platoon. Both the STAFF INT OFFICER and OMT/s can be co-located at the Brigade main CP.

The TACHUMINT team can also help the subordinate battalions to acquire good HUMINT capability when they collect intelligence as per the infantry Bn collection plan .In this instance the teams work in DS. Here the OMT which controls the teams will be now co-located with

the Bn STAFF INT OFFICER cell. In addition to reporting to this STAFF INT OFFICER about the teams collected information it also reports to the STAFF INT OFFICER of the Brigade located in the Brigade main CP.

We have defined the C2 relationship. Now we set up an exercise to keep the teams ready for any mission.

MISSION BRIEFING: TACHUMINT teams. OMT briefs them about target-specific targets set for each platoon—to collect info against target. Collection plan.OMT prioritizes platoon tasks. Ensures each platoon works in concert with the other, in harmony, keeping overall collection plan in full perspective. Platoon commanders, OMT and STAFF INT OFFICER of Bde present during briefing. Platoon leaders told to share good TTPs among them. Thereafter inspection was carried out. Equipments, weapons, communication sets. Combat rehearsals were carried out.

Then the tasking began. A role play scenario. A model village supposed to be the sanctuary of insurgents. Locals were soldiers who were asked to behave like locals, apprehensive of the soldiers in the teams. The TACHUMINT teams were casual, unobtrusive but always prodding along carefully with mission requirements in mind. They were briefed clearly about targets, about intelligence requirements, which requirement was priority and the fact that all teams need to be in harmony while making a situational understanding template for the commander with the acquired information. The soldiers were now in contact with the ‘’locals’’...Some asking slanted questions, some building up rapport and others engaged in unobtrusive tactical questioning, elicitation and gossip with intent to acquire pertinent information. Attempts were made fully not to be threatening, to be genial and build up an atmosphere of trust...Projecting an image of friendship, protection. They were respectful of the village culture, deference to women folk and avoiding questioning them if possible and friendly with the children, often offering chocolates. In the backdrop intent is also there to segregate the locals into who supported the forces and who didn’t. To find out if any were particularly offensive or held the forces in disdain. They were alert to note the behavioral indicators...If anyone was trying to avoid eye-contact, or if being overly-helpful or if avoiding discreetly and moving away from the crowd etc.

After the exercise is over they are back at the garrison. Using the communication equipment and hand held equipment they reported their findings to the Int Ops cell at the Brigade STAFF INT OFFICER Section.-The OMTs too benefited from this exercise in now that they have experimental data to practice upon. Data to screen, analyze, correlate, and use link analysis to discern linkages between activities and contacts made. Using all these follow on exercises were set up for the next day

An Operational Management Team Collates Data Gathered by the TAC HUMINT Teams.

To achieve synchrony, while the TACHUMINT teams continued with their exercise the OMTs and Brigade STAFF INT OFFICER section were busy .The OMTs screening data,evaluating,analyzing,forwarding to the Int Ops of STAFF INT OFFICER section, the STAFF INT OFFICER utilizing the Int Ops section to coordinate the overall collection effort. The data sent in by the OMT was broken down into manageable chunks, formatted, indexed, correlated with source registries, stored in databases for easy retrieval and disseminated to intelligence planners in the Bde. A computer system was created linked with this database wherein all source-lead development reports were stored, link-diagrammed to infer an understanding of all relationships between HUMINT sources in the Bdes area of interest. Not only that a clear picture came into being about the source-leads and the entire source network. This will assist greatly in the problem of deconfliction.

All this goaded the Bdes intelligence collection effort in the right direction and in keeping with the Commanders prioritized intelligence requirements. To further the situational understanding at all levels throughout the Bde a portal on the Tactical LAN or webpage can be set up with all information acquired so that all intelligence personnel and reconnaissance troops can view them ,if necessary take out required data, also update them with any new information (in conflict situations change rapidly, intelligence drives ops, ops in turn generate further intelligence requirements).Not only intelligence personnel but maneuver control, system personnel can also view all the intelligence and plan accordingly.

The CI element in HUMINT Ops.

Force Projection facilitating interim combat HUMINT/CI enabled R&S Team

OMT Functions:

Conduct surveillance planning.
Coordinate surveillance support.
Produce the surveillance plan.
Brief the surveillance plan.
Ensure recovery of surveillance personnel and equipment.
Provide oversight of surveillance debrief
Review reporting.
Provide analytical input. Disseminate reporting.
Brief results of surveillance mission..

Direct employment of HUIMNT technical operations (HTO) and CI
Equipment, as required.

The usual reconnaissance patrol or Long range surveillance or any R&S asset deployed to collect information usually does so in the standard zone, area or route reconnaissance pattern. The patrol usually has self defiance capability, can move and dismount rapidly and is effective in so far as surveillance or recce is concerned.

The battlefield has transitioned from a deterrence based profile to force projection profile. That is to say that once an area of operations is identified so that the strike forces (Brigade) may move in and engage in operations, a combat reconnaissance team can be sent in to:

Conduct the usual:

Reconnaissance and surveillance

AND

Conduct a brief intelligence preparation of the battlefield

Conduct HUMINT ops

Conduct CI ops

All these being done so as to develop a situational understanding of the area of operations , the threat assessment (Leadership,OB,strengths,capabilities,TOE) including the human terrain comprising the locals, other communities, the local village government so that the incoming strike forces can optimally target:

Physical as well as behavioral targets. That is kinetic or non-kinetic attack modes to be deployed with precision.

Thus the usual reconnaissance team is now supplemented within CI soldiers and a separate HUMINT platoon from the same brigade works closely with the CI augmented R&S troops. The inclusion of CI assets beyond the front line deep into enemy territory considerably heightens the HUMINT collection. Add to this the HUMINT platoon advantage and we have a interim combat team capable of defending itself with rapid mobility and mounted/dismounted ops capability and

also capable of CI and HUMINT collection apart from reconnaissance and surveillance. Thus here we have all the three ISR assets working in harmony and controlled by HQ which is in effect an organic Bde staff section comprising of intelligence officers from the Brigade itself. This STAFF INT OFFICER cell conducts all HUMINT/CI ops management, deconfliction, exercises technical control, analyses and forwards all intelligence to the Brigade and throughout the command.

STRUCTURE:

The reconnaissance team equipped with armored recce vehicles can number three platoon per squadron, ,4 recce vehicles per platoon,2 man crew for each recce vehicle,3 man squad per recce vehicle and one linguist augmentation who is a CI soldier.

Integrate Intelligence Training into Unit Training Plan

There are two types of unit intelligence training: (1) internal training conducted within a unit intelligence section, intended to further refine and expand the section's proficiency and capabilities; and (2) external training directed toward non-intelligence personnel within the unit, intended to orient them to threat capabilities and activity, familiarize them with intelligence section capabilities, and facilitate the integration of Intelligence into operational planning and execution.

Steps:

- Review units mission.
- Review units operational training requirements.
- Develop an internal training plan.
- Develop a unit operational intelligence training plan for non-intelligence personnel.
- Track training progress.

APPENDIX

****Keep the following method of classification/numbering in mind when handling intelligence requirements:***

Enumeration. We must create a system of numbering out intelligence requirements not only to highlight the priority level but also to keep a close track on the progress. While checking or reporting which requirement has been satisfied during collection the HUMINT operative simply puts the code in parentheses after each paragraph of information. The HUMINT collectors should be handed down all the requirements in a simple format to avoid confusion, and to be both general and specific as the case may demand. For example the focus can only be on the entire supply department where we are looking for corrupted officials. Or we could be more specific by focusing on sections/depts. of interest within the supply deptt.Now we can proceed as follows:

First we write down the PIRs and IRs.

Here PIR#1 is Supply officer's corruption

IR#1 the officers mess where transactions take place.

Of course we can have several PIRs and IRs and even more SIRs.

We may use diagraph—combination of two letters.

AS1000 meaning Army Supply dep't with 1000 series, the series can accommodate numerical codes assigned for corrupted officials (top level—say 1001 is the OC, 1002 the 2-i-c etc), ASTAFF INT OFFICER000 (middle level) and AS3000 (enlisted).

We can be more specific: We are focusing on terrorist group involved in drugs and ransom taking to generate income for terrorist activities: So very first the main PIRs:

PIR#1 TERRORIST FINANCING

IR#1 Drug trafficking

SIR#1 Drug production

SIR#2 Drug safe houses/warehouses

SIR#3 Drug transfer

IR#2 Hostage taking

We can use diagraphs:

TF1000 terrorism financing (general expression)

DA1000 Drug activity

HK1000 Terrorist hostage taking history and TTPs

(Above two are general classifications with main TF1000)

Now let's be specific:

HK2000 Kidnapping history of suspect group

HM3000 Modus operandi of past kidnappings

DA1000 is drug activity with the 1000 to incorporate suspects assigned codes. This is a general definition. Let's be more specific:

DP1000 is drugs production with code

DSTAFF INT OFFICER000 is drugs safe houses with code

DT3000 is drugs transmission channels with code

Similarly we break up Hostage taking.

APPENDIX

Intelligence Support to Targeting

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.

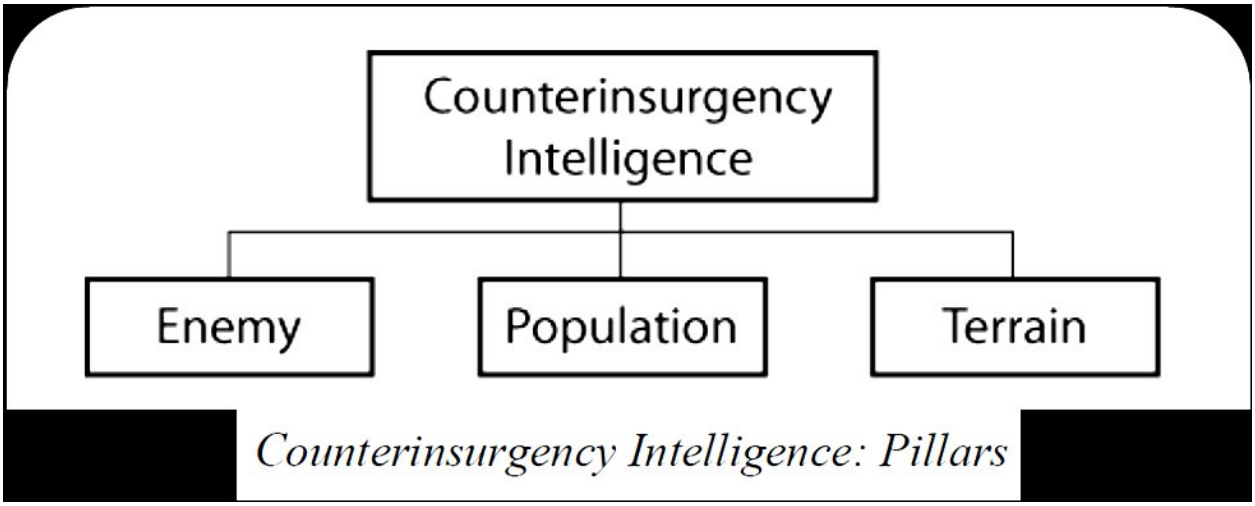
1. Stress should be given to the fact that tactical company and platoon level units conduct operations with a high degree of success and hence higher levels of command must push intelligence staff and information down to lowest points of collection (initial points) , that is the company/battalion levels.

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.

NOTE: Other details on how to create an organic intelligence unit at boot-level , establishing target folders , merging HUMINT and CI capabilities to assume a tactical HUMINT capability , source operations , **force protection (VERY IMPORTANT TO AVERT DANTEWADA AND KASHMIR CAMP FIASCOS) ,** unit protection , personnel-physical-information security , Counterintelligence tactics , techniques and procedures , HUMINT tactics , techniques and procedures , intelligence requirements and collection management , intelligence cum force projection capability(interim-combat team with organic ISR assets) , company support intelligence team creation , ES2 concept (every soldier is a sensor) , military police intelligence operations , HUMINT/CI doctrinal deficiencies and recommendations, need for professional military intelligence education and recommendations and other topics are detailed in 4 available books by the same author.

KESHAV MAZUMDAR

ATO

APPENDIX

TACTICAL HUMINT

HUMINT is collected information which we term positive intelligence after processing.HUMINT collectors access human sources and multimedia to gain information about enemy intent,composition,disposition,capabilities,table of order and equipment, command control nodes, centers of gravity,leadership,personnel—this is also called Order of Battle when conducted prior to a combat situation. The Commander specifies his intelligence requirements explicitly and going by these requirements , prioritized , human sources,informants,and other human elements possessing information compatible with the said requirements are utilized by application of specific techniques like tactical questioning,debriefing,document exploitation, eliciting and interrogation and reconnaissance and surveillance. The HUMINT collectors are not intelligence operatives with general intelligence education and training but specialists.

Counterintelligence is also a collection oriented discipline like HUMINT but not an intelligence discipline in the strictest sense. It is concerned with enemy intent while HUMINT is concerned with collection part only so as to satisfy Commanders intelligence requirements in order to answer certain information gaps.CI attempts to prevent sabotage,assassination,terrorism,subversive and enemy intelligence activities , deny the enemy access to installations and sensitive information , acts as a protective shield for the Commander by supporting OPSEC and force protection and acts in an advisory capacity recommending countermeasures to enemy intelligence activities.CI is a protection component in the Commanders repository of defensive tactics and techniques and CI also protects the intelligence cycle. Several definitions exclude personnel, physical, document or communications security programs from CI purview , but on close inspection it will be seen that CI invariably is resorted to while implementing force protection and denial/deception measures (information warfare) thus bringing in play the security aspects of personnel , physical,documents.CI support tio physical security , infrastructure, technology protection, military security,HUMINT –all these some way or the other involve those elements that are kept out of general definitions.

Definitions can be very confusing, may render doctrine imperfect and lead to redundancy. For example the Army ten ds to maintain a general perspective on threat—statements like our forces are prepared to deter /attack/defend against a wide spectrum of threats, ranging from criminal

activity in our jurisdiction which may abet our main enemy, terrorism , subversion to small wars, wars and battles. Now this generalized concept is fine in that we can have several security programs, each tending to one specific threat type in the entire spectrum. But the disadvantage in this approach is we cannot focus on the main threat, say terrorism, and as security concepts like force protection, deception

operations, physical security, military security,etc all have certain elements in common we land up with redundant programs designed to handle these security concerns. For example antiterrorism and force protection both have in common physical security as a passive defensive subcomponent where the installation critical points are protected after vulnerability assessments and red teaming. The same subcomponent is the major component in a physical security program. Thus there occurs good redundancy if we do not have a focused view of the threat and counter threat measures become diffused over the broad spectrum.

The same goes with the definition of intelligence and CI. Or rather I should say the general p[perspectives held by most Commanders and even intelligence officers.

The main idea is to remove uncertainty and gain a decision advantage. This should be the prime objective of the Commander.HUMINT and CI are both shaping operations but with a critical difference.HUMINT shapes the Commanders view of the battle space by providing him accurate intelligence about enemy order of battle. Plus other information requirements when ops are in progress.CI on the other hand penetrates the enemy commanders decision cycle and shapes his views ‘’like the way’’ our Commander desires by denying the enemy commander access to our operations, plans and information systems , and using offensive methods like penetration , infiltration and also denial/deception operations. Both shaping operations have one thing in common as goal. To act as force enabler. To heighten the Commanders situational understanding. In other words to gain that ‘’decisive ‘’ advantage. **.To get a ‘’positional’’ advantage.** HUMINT shapes the "Blue" forces' understanding of the "Red" forces while CI affects the Red forces' knowledge of Blue forces.

HUMINT shapes the understanding of the ‘’Blue forces’’ with respect to the ‘’Red forces’’ while CI does the reverse. True both use several techniques which are in common like interrogation and other low level source operations but going by what has been discussed CI is not HUMINT and not in the least a subset of HUMINT. Being a subset would mean CI operations would be counter-HUMINT only. But CI looks beyond that, by conducting offensive operations, denial and deception operations , exploiting enemy intelligence activities ,neutralizing them through collection of evidence and subsequent prosecution for national security crimes, and supporting tactical and theater operations by feeding inputs to the decision cycles. Thus we see CI goes far beyond Counter-HUMINT operations.

Interrelationship

CI also provides positive intelligence about the enemy as a byproduct of its operations.CI and HUMINT operations overlap in that very similar techniques are often used. In fact in tactical operations a mix of HUMINT and CI operators plus a linguist carry out tactical HUMINT operations where the roles of both are more overlapping and confusion arises when either may operate like the other. We should not always justify HUMINT source operations..this leads to the mistaken impression that CI only lends support to HUMINT and has no other function and that HUNMINT and CI are the same thing.NO.Whereas HUMINT focuses on the enemy's organization,composition,capabilities and decision making without any focus on the intent of collection , only collecting all require information laid down in the commanders prioritized intelligence requirements order , and reporting it through proper channels (and here full stop) CI will go much further , exploiting , neutralizing the enemy intelligence activities or doing both…CI is concerned with enemy ''INTENT''.HUMINT focuses on the enemy's decision making cycle to gain information for the Commander whereas CI attempts to ''INFLUENCE'' that decision cycle and shape it the way we want it in order to achieve winning objectives. Thus the HUMINT operative tasking end after detecting and identifying enemy intelligence activities while the CI agents tasks begin afresh.

From all this discussion we can derive two things:

1. HUMINT and CI are different.CI is not a subset of HUMINT.

2.As HUMINT and CI have many similar lines of operation , if both can be combined to satisfy tactical requirements ,(during theater or national-level requirements they can revert to individual role-this capability must be retained) , we will have an intelligence operator who will be more versatile,adaptable.and can confirm easily to all army requirements at the tactical level. Tactical intelligence formations can execute this tactical HUMINT asset (the operator) to satisfy commanders requirements. Merging the capabilities of HUMINT and CI results in a task organization of skills for the Commander—definitely an improvement over either HUMINT or CI enabled operations. Tactical HUMINT operations are most suitable for developing and maintaining an excellent informant/source base that provides timely, specific and accurate information. Tactical HUMINT operations combine both HUMINT and CI techniques and together with linguist assistance , are more capable of developing and maintaining contacts than only HUMINT or CI ops.For example , the Tactical HUMINT team comes across few individuals of interest near the forward area , the HUMINT operators conduct tactical questioning to extract information of intelligence value and then pass them over to their CI

colleagues for further interrogation if they discern any information of interest to the CI operators. This can be switched to and fro and the application of the combined faculties of both results in more refined, relevant and timely/accurate information. If the individuals are of the witting type or have voluntarily offered to deliver information or are community members sympathetic to the forces, then they can be inducted into the source repository by establishing rapport/giving incentives etc and then later their assistance taken for more information. Tactical HUMINT teams can act as mobile interrogation teams at forward areas, quickly disposing off sources after tactical questioning and interrogations, thereafter detailing escort for those who may render more information or who, it appears are suppressing tactical information, sending them to detention centers and collocated interrogation areas near forward areas or in the rear. The standard procedure of detaining and escorting to rear interrogation areas is hereby bypassed as in this procedure , the time taken to assess , detain , segregate , and transport to rear areas can negate the availability of timely intelligence—intelligence is highly perishable ,. Especially combat intelligence, where time is of essence.

Hence as the repository of sources grows, the quality and content of available information is enhanced and for the commander tactical intelligence, most of the time, is at his fingertips. Compare this to the situation where earlier, HUMINT or CI operations had to be complemented by intelligence from theater or national agencies, and it so happens they cannot provide real time, ground intelligence always for combatant commanders.

The soldiers will be given language training, Basic CI training, operational debriefing training so that as and when required they can shift from tactical to operational briefing to CI functions. **The focus of training should be cultivating the capability to conduct contact and informant operations, recognize information of CI value, and execute tactical questioning of civilians, and screen EPWs and detainees with the assistance of an interpreter.**

Tactical HUMINT team functions:

1. Tactical tasks with Language training
2. HUMINT Ops=Strategic Debriefing
3. CI

Here it should be stressed that intelligence nowadays is tactical—the focus should be at tactical level as soldiers fight wars nowadays more than battles. Small-wars in fact. Hence the dire need for actionable intelligence/tactical intelligence. Here the players are combatant commanders who must move swiftly in their maneuver and strike decisively. Higher echelons are there for planning, average intelligence support, but it is for the ground based Tactical HUMINT teams to do most of the work. And they do it—as their composition is quite what the modern day warfare demands.

CI/HUMINT

Counterintelligence functional services are provided to promote the Commanders situational understanding.

- Define and analyse mission
- Execute CI Surveys
- Prepasre a brief on CI Awareness
- Execute CI Vulnerability Assessment
- Execute CI Threat assessment
- Execute CI Inspections
- Execute CI Reviews
- Execute CI Evaluations

Conduct CI support to HUMINT activities

Identify, exploit and counteract foreign intelligence activities across the full spectrum of HUMINT activities. CI activities include, but are not limited to, identifying friendly and hostile capabilities and vulnerabilities; providing CI review of HUMINT activities; conducting CIdamage assessments; providing support to Counter Espionage (CE) investigations; conducting and/or assisting in asset validation by physical and technical means.

Perform CI/HUMINT operational planning.

1. Supervise the preparation of CI products, as required.
2. Obtain necessary approvals.
3. Supervise CI support to HUMINT operation.
4. Supervise asset validation procedures.
5. Conduct post-mission analysis.
6. Disseminate required reports/products.

CI/HUMINT Collection management

The CI/HUMINT officer/JCO will match the requirements with the collection assets in hand , checks availability , usage by other adjacent units , deployable possibilities etc and then determines the best collection plan.

- Receive prioritized intelligence requirements from higher headquarters or collection manager , conduct analysis
- Create the collection plan
- Study all CI/HUMINTcollection assets available and match them with the requirements
- Decide on the course of action to fulfill collection objectives
-

Docex

The CI/HUMINT officer/Jco must be acquainted with the exploitation setup and the units exploitation SOP so that he may, after receiving, accounting and sending the captured materials he may be able to follow-up for results and give future feed inputs to the exploitation cell/agency.

- Understand exploitation agency infrastructure
- Identify exploitable materials
- Categorize them as Biometric Examination or Forensic Examination.
- Take possession of exploitable materials
- Account for and categorize exploitable materials
- Prepare catalogues
- Dispatch the materials to exploitation agencys custody
- Followup with the agencies for results
-

Identify orders of battle in given Area of operations

Identify Ground military attack and defense capability, Air-defense and attack capability, naval capability and all associated military weaponry systems and equipment, such as ground combat systems, antiaircraft systems, naval vessels, etc.Study the enemy infrastructure and locate/identify the keys areas.

Intelligence support to Targeting.

This includes identifying enemy targets , both high value and high payoff , nominating in order of priority , recommending kinetic or non kinetic attacks, and thus assist the Commander to destroy, neutralize or exploit the target in a manner which is in line with the units mission and in keeping with the Commander and his staffs requirements.

The Unit intelligence supervisor who controls the target intelligence collection and associated ops/recommendations to the Commander must be as thorough as possible, evaluating all factors and intelligence inputs carefully, studying imagery data and compiling and organizing target information efficiently so that while nominating to the Commander and making recommendations there is absolutely no ambiguity. Target descriptions including composition, location, importance, imagery, graphics, construction—all of these are spelled out correctly and particularly for HVTs/HPTs their location, significance, all associations determined and influence with respect to the leaderships decision cycle/battle space situation.

Identify:

- Targeting Categories
- HVTs/HPTs
- Areas of Target value
- Build a list of targets
- Locational factors of each target
- Associations of each target(COIN)
- Social circles of each target (COIN)
- Assess target significance/value
- Determine whether to employ kinetic or non kinetic attack
- Contribute to attack guidance
- Assess effect of removal of targets on battle space
- Create and maintain target folders
- Decide on target intelligence requirements
- Create target nomination list
- Combat assessment
- Update target folder based on combat assessments.
- Contribute to IO
- decide on restrike options

Evaluate the Threat

Determine threat intent, capabilities, vulnerabilities, possible courses of action and the most dangerous course of action.

It is of prime importance to study enemy activity and indicators to assess his capability to attack, defend, withdraw, reinforce. Focus on the intelligence gaps and this focus can determine the direction of collection of intelligence. Enemy activity patterns should be studied.

Factors influencing the intelligence product are the time available for collection, assets available, unit size, the intelligence requirements, AO features and the mission. The enemy, terrain, weather, local populace are taken into consideration. Identify:

- Enemy Intent
- Enemy Capability
- HVT
- HPT
- C.G.
- Critical areas: Capabilities,Requirements

APPENDIX

TACTICAL QUESTIONING

Collecting Information

Soldiers patrol the same area day after day. Sometimes they go in for deep area patrolling and reconnaissance. All this is done with the intent to collect combat information.In any

operational environment soldiers should always be primed , alert to collect information.Of particular mention here is te word ‘’change’’.While patrolling the soldiers may discern a ‘’change’’ in normalcy of the surroundings. While studying the surroundings , like the people,terrain,infrastructure the soldier should recognize any changes in the environment.Often than not these changes are important indicators cof enemy activity or intent.The soldier may not be able to find out the reason behind the change , still it’s very important he report it to the intelligence personnel. Soldiers should train themselves to become constantly aware of conditions such as

- Armed Elements: Location of factional forces, minefields, and potential threats.
- Homes and Buildings: What is the condition of the roofs, doors, windows, lights, power lines, water, sanitation, roads, bridges, crops, and livestock?
- Infrastructure: The presence of functioning stores, service stations, etc.
- People: Numbers, sex, age, residence or displaced persons, refugees, and evacuees status, visible health, clothing, daily activities, and leaders.
- Contrast: Has anything changed?

If everyone is involved in the collection of combat information, then everyone must be aware of the information requirements. All soldiers who have contact with the local population, routinely travel within the area, or frequently attend meetings with local organizations must know the information requirements and their responsibility to observe and report.

While handling detainees and EPWs keep the following in mind:

1. Segragate the detainees and EPWs based on nationality , sex , profession , ethnicity (civilians) and rank , insignia , and regiment (may be belonging to enemy intelligence unit , thus game for special interrogation)

2. While searching the person of the detainee or EPW search thotoughly.Keep separate the records of documents , seized equipments and weapons(capture tags).Describe all documents,equipments and weapons as completely as possible.This is not DOCEX or Captured equipment exploitation in its entirety—that will later be done by trained HUMINT personnel and with help of technical assistants.What is being done here is tactical exploitation , just like tactical questioning—on the spot intelligence extraction.

3. Intelligence is perishable and combat intelligence is highly perishable , action is required as soon as possible and for that the intelligence must reach the targeting platform without any delay.But there are procedures.The prisoners and detainees who are felt will yield more information on further questioning must be moved as soon as possible to the rear where interrogators are waiting.Bear in mind that with time the detainee/EPW emboldens , the initial panic which he had on point of capture wears away , he gets time to think and also harbors escapist thoughts—escape from captivity.We are here talking about the duties of secondary collectors , the line troops who must move them fast to rear after ascertaining that they do have information of value.There are mobile interrogation teams to handle cases right on the spot at forward areas and copmposed of a mix of HUMINT/CI but that is ***tactical HUMINT and will be dealt within my book on Counterintelligence.***

4. Kep a tab on the detaines , EPWs and all others so that they do not communicate with each other.

5. Remember the personal safety and protection of all detained for questioning can be a cause for concern under certain circumstances and hence they must be safeguarded.For example someone from the line troops may vent his personal anger on the enemy by attempting rough handle the detainees or prisoners.Sexual harassment is also an issue.Whatever be the case , they must be treated humanely.

Key Considerations for Talking

- You must be aware of the existence, nature and type of threat in your area and the vulnerabilities of the protection measures taken by your commander which are liable to be tapped. Overall you should know the force protection measures taken by your unit.

- Be careful about the local culture, traditions, customs.

- Your body language should project a friendlier flavor, not an intimidating one. Point weapons away from the accosted person.

- Talk to people in normal surroundings.Dont lead them to an isolated area, an alley or any place which will make them suspicious. Always be polite. Remove sunglasses.

- If you are speaking to a woman know local courtesies.

Questions

Questions should be so structured so as to be simple, straightforward, should open and maintain the conversation, should start with an interrogative, and should prompt a narrative answer. Interrogatives are what, why, when, who and where. Questions should not be closes provoking only an ‘’yes’’ or ‘’no’’ as answer but should be ‘’open’’.Avoid asking questions that are confusing. Characteristics of open questions:

- Act as an invitation to talk.
- Prompts the person to answer comfortably and feel encouraged to continue with the conversation.
- Not too specific but broad in nature.
- Encourage discussion.
- Creates a situation favorable for the soldier to be the listener(and observer) for a major part of the conversation.
- Does not cause the person to feel intimidated or threatened.
- Invokes curiosity of others and allows them to get involved in the discussion spiritedly.
- Gives the person the opportunity to tell his opinions, his judgment, what he feels is important, what he feels should be done.
- Should invoke a conversation, not a question-answer scenario.

Be subtle, don’t just jot away on paper the answers –that is not conversation and always be friendly, cooperative, observing him carefully but not arousing any suspicion, studying his body language and be courteous and reserved.

Questioning to Fill Out the Capture Tag

You are manning a check post or roadblock..Before being deployed to do so your unit commander has briefed you about the intelligence requirements as per current mission. The Battalion prioritized intelligence requirements lead to the generation of intelligence requirements for each company and subunits. These intelligence requirements as spelled out to you will guide you in framing the questions to be asked of individuals at the check post/roadblock. Once you, the soldier, have screened and detained a person categorized either as a detainee or EPW you must now obtain all possible details from him so that on subsequent questioning/interrogation of the person by the HUMINT or CI agent, the latter is well prepared initially with the information you have supplied. You must fill out a capture tag which will facilitate further questioning/interrogation. The capture tag must include:

What is your job? What is your speciality? Are you a combatant? If so what is your rank, number and unit? Who are in your chain of command? Whom do you report—that is who your immediate superior is? What is the mission of your unit? Are you a civilian? Then why are you here? Who is your immediate boss and what is the name of your company? At the time, place and point of capture, detention what was your immediate mission—that is to say why were you there and what were you doing or what were your plans? Were you supposed to conduct any mission/job when you were captured/detained? What are your future plans and what is the future mission of your unit/company? You might note he is carrying documents, maps, identification papers; photographs.Here is where you might find things out of the ordinary. The map might be of another place or even this place: Why are you carrying this map? The photo/s might be of someone else: Who is this person and why are you carrying his photograph? The ID papers may belong to other persons and hence you ask him why is he carrying other peoples identification papers and why. And where are these persons as they are in a disturbed area and that too without identification papers. All these exploitable documents can now be handed over to the MI section together with the detainee/EPW.

Remember your questions should be guided by your unit's intelligence requirements and as briefed to you but on no count should the person being questioned get a whiff of these requirements or your mission. Everything should be done in an atmosphere of normal conversation.

Example Questions

Questions must be framed in such a manner so as not to elicit vague or misleading answers. They should be direct, pointed but at the same time broad so that the person being questioned does not misinterpret it or has any room for maneuver. For example the following questions were designed for soldiers manning check posts/roadblocks. Modify them to accommodate EPWs/detainees, local population as per your mission, situation and unit requirements.

• What is your name (Match this with any identification document found on his person) Cross-check with CI White list, Black list and Grey List)

• Where do you live and full address, where were you going and why, how did you arrive here. From here to your final destination point—what will be the route and why? In what way is it safer or convenient for you? Who will facilitate your journey? That reminds me, who facilitated your journey till here, financially or otherwise? (All these must be specifically answered or obtained)
• What is your present occupation, your specialty-if any and your qualifications (see if he has any technical expertise)?
• What was the type of physical terrain you travelled to get here? During your travel what all obstacles you faced and how did you manage to overcome/circumvent them. While travelling did you observe anything out of ordinary in your surroundings? Or any unusual activity?
• What currency are you carrying and how much? What is the money intended for (if found to be a big sum)?
• Can you name anyone whom you know personally who is averse to Indian security measures/ops here in this area? On being answered immediately follow with ‘’who else’’.Do you know or are you aware of the nature and type of any anti-Indian security operation/any other activity here or anywhere else and dates or time of such activities? Can you tell me the reason for our forces to be here? Do you support our activities?

DO NOT’s

• Ask questions which might reveal your intent or which might make him aware of your units mission, intelligence requirements.
• Jot down answers before him.
• Don’t resorts to quid-pro-quo.They are not permanent sources to be given goods/money in exchange for information and neither are you an intelligence specialist. The same goes for EPWs and detainees.
• Do not resort to coercion. You may be reported to social media. Or the police. Remember we are all governed by Geneva Conventions.
• If you are handling EPWs and detainees escort them to the interrogation center as soon as possible. You are only supposed to ask basic questions to civilians in conversational mode. Yes if situation is fluid, like in battle and yu accost suspicious civilians you may resort to interrogation based tactical questioning, but only to ascertain if they are of interest to HUMINT/CI personnel and carefully examine any captured documents. In such cases escort them quickly to detention centers from where the MP will take them to interrogation centers. • Pay money for information.
• Do not be so cooperative so as to tell them their rights that can be handled later. First the information from them.

Reporting

For tactical operations, there are four levels of reporting which assists the Unit intelligence section to factor in all useful tactical information gained during the

small units activities in the overall planning of the mission (and also update ISR planning):

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

· Normal reporting

· Information during normal debriefing sessions by the intelligence officer.

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

Document Handling

When there are documents on the person of the detainee efforts should be immediately made to:

- Classify them
- Seize , Impound or return them
- Determine if they contain information which can be exploited further by trained intelligence personnel (DOCEX).

Remember that any document, even though it may seem irrelevant on first sight , may on close inspection reveal information of interest , might satisfy intelligence requirements and with other seized documents give a bigger picture of enemy intent.

Classification:

Documents can be Personal such as letters, diaries, photographs, flyers posted in cities and towns, etc ,Identity such as identity cards , passport, drivers license , ration cards or Official such as documentation government/military information , for example military books , field manuals, military reports,files,maps etc.

CED (Captured enemy document) is a piece of recorded informnation seized from the captured person belonging to the enemy forces or any civilian in collusion with the latter.We can also name our own military documents CED that were in the possession of the enemy.DOCEX of such documents can rev eal what they know about us , or if anyone was involved on our side in transferring these documents to the enemy then we are alerted to the fact and going by the nature of the document or its origin we can put our CI agents to track him down.CEDs can be

found on the person of EPWs/detainees , abandoned military areas , on the bosies of killed enemy personnel , old enemy command posts , destroyed enemy forward tactical headquarters.

A CED is defined as any piece of recorded information obtained from the threat. CEDs can also be US or allied documents that were once in the hands of the enemy. CEDs can be found almost anywhere; some locations include abandoned training sites, old enemy command posts, deceased persons, cafes, town squares, or in the possession of EPWs/detainees.Written or typed material, drawings, audio, and/or video recordings, computer disks,etc can constitute the content of a CED.

Once you have critically studied the CED you have to decide on three actions:

- Return them to the owner as they are very personal items and do not contain any military or governmental information

- Impound the CED with the intent to return them later as these documents being of personal nature contain information pertaining to the military but which after examination is found not to have any bearing on current situation or having any affiliation with the enemy. Still they will be sent for DOCEX and if the initial assumptions are true , they will be returned.

- Confiscate the CED as it contains military or governmental information (all official documents)

Every confiscated or impounded CED must be tagged and logged before being transferred for DOCEX.

The capture tag should contain the

1. Unit details who captured the CED
2. Location of capture : Grid coordinates
3. Time and date of Capture
4. Identity of the person from whom it was captured including brief description (Rank , unit etc)
5. Prevailing circumstances under which the capture was made
6. Description of the CED

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 Admiral Peter Kikareas (NATO, presently retired) 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 belowmentioned course site is offered only to Security personel around the Globe.

Intelligence/CI Course webpage : www.securityantiterrorismtraining.org/course.php


TIOCC
NTCORPS
Intelligence Drives Operations