Bn Int Platoon - 1 Coy Int Cell

Battles , Force Protection & Intelligence : What is apparent & What is lacking actually.

ATTACK THE NETWORK PLAN

May 6th, 2017

TARGETING IN COIN

Keshav Mazumdar ATO CMAS

Kinetic Targeting is a process by which physical action is taken to kill/capture insurgents or for that matter any enemy in the area of operations in order to negate their activities/operations in the AO.For example HUMINT reports bring in information about an insurgent facilitator of IEDs supply.Kinteic Targeting , that is killing this element severely affects the IED supply thus limiting the usage of IEDs by the insurgents.Here it is very important to choose carefully the targets.They should be critical nodes in the network , destruction of which will hamper the overall operations of the network , not just cut off one single line of operation.Thus targeting C2 nodes , critical lines of communication and logistics , important couriers and informers of the enemy , prime facilitators from among the local populace , HUMINT agents from among the local populace and anything or anyone close to the or collocated with the perceived centrer of gravity of the network will in effect disrupt enemy operations as well as planning severely.For example we have identified and located a high profile insurgent and a drone attack results in his elimination.Thus we have successfully removed a node in the network.Now if we study the second and third order effects of this attack , that is the resultant action on his colleagues or men under his command and the effect on the local population(our HUMINT and CI people keeping a tab on enemy movements, enemy suspects and activities of local suspected sympathizers , facilitators) we get further leads for further targeting actions.It couls be , for instance , that after removing this critical node there is a flurry of activity in the local community among a select group of people , or maybe demoinstrations are held thus pinpointing the actual sympathizers(these can now be included in non-kinetic operations) or the activity of insurgents themselves which become observable and thus amenable for intelligence action.

Conventional war sees both adversarys attempting to utilize the entire spectrum of combined arms warfare to:

1. Annihilate the others forces

2. Cause severe attrition to erode the overall enemy strength and projecting capability so as to penetrate our defences or mount a piercing attack or in intelligence terms , be deprived of projecting interim intelligence enabled combat troops. same time attritting the adversary's strength and their ability to project force.

Coming to asymmetric warfare like guerillas , insurgents and terrorists here attrition is not a solution as most of them , going by Maos principle , are intent on conserving their forces—that is strength , capabilities as they are far outnumbered in and they cannot afford to take in more casualties by foraying enmasse into enemy territory like conventional forces or for that matter projecting their force is not an option for them.They carefully choose their targets and the location where they will deliver the attack.All this done by small line squads while the majority of the insurgents stay safe at the bases.

Here is where we can arrive at a very important inference.If the insurgent must conserve his forces which means as his primary objective is to cause harm to the security forces without exposing himself unnecessarily , attacking from deep cover , or ambush , he needs pewrfect information about the nature , identity and location of his target/s.To this end intelligence capability ios critical.If he employs his own intelligence assets , which are very very limited , his own men who can keep an eye on troops movements from afar or from a top vantage point—and that is quite risky some times , the insurgent leadership then turn to their main resource base , the local populace.The limited HUMINT agents of the insurgent group now recruit sympathizers and others who support their ideology , or those who bear a grudge against the local administration , police and the security forces themselves and now these very innocuous looking people of the local community in the AO become the eyes and ears of the enemy.As per Mao's principle , we can infer the insurgents should conserve this HUMINT capability in order to conserve their forces.This further leads to the fact that they will also protect their informers and sources and like a professional intelligence organization will surely conduct secret meetings to indoctrinate them on security principles , how to handle their captors if caught by the security forces and other psychological instructions.

Whatever be the case the local populace is and should be the main target of the Army intelligence apparatus —detect , identify and locate the HUMINT elements. History , Malaya , Philippines , Iraq , etc ..has proved time and again that a successful insurgency emerges only with the support of the local population.

Hence comes into the picture –non-kinetic targeting.Now it is clear that the insurgents will do everything possible to keep the population on their side.If not the entire local populace , well all those who sympathize or believe in its ideology or others.As for those elements of the population who are some way or the other disinterested in the insurgency movement or even averse to it , these people are kept in leash by the insurgent leadership.Intimidation , fear , torture and even killing—these tactics are resorted to.But generally the elements of the population who are so labeled as averse to the insurgents ideology prefer to keep quiet.These people must be identified by our intelligence personnel.As they are part and parcel of the community they can offer valuable intelligence on the elements of the population who work for the enemy.They are the best ones suitable for surveillance , static observation of the neighbourhood , getting good access and placement to suspects (after transmittal of the idea that they are pro-insurgency) , reporting on strangers in the village , attending propaganda meetings and hate-seminars , and knowing the entire terrain very well so as to advise the security forces during intelligence preparation of the Area of Operations.

That said , the Army should and must wage a full scale parallel war with the insurgents in controlling and influencing the minds of the population in their favour.This love/hate triangle is in fact the most important mission objective.You control the population , you know the local informers and logistical supporters of the enemy.Also the safe houses , staging areas and all clandestine meetings in the area.Going a step further , detaining such individuals and interrogating them , or more the better keeping them under tight surveillance using those friendly elements of the population you can now detect and identify their enemy HUMINT contacts.Further

surveillance or arrest and detention followed by interrogation can lead to weapon caches , staging areas , other enemy personnel concentration points , transit camps , bases—in short you get nearer and nearewr to the insurgent center of gravity.

This parallel war is in effect information operations.Information operations , such as periodic or random announcements by the loudspeaker and other media enabled platoon , PSYOPS platoon , coupled with community development programmes such as road repairs , distribution of food and sweets to children at regular intervals in primary schools , helpinmg in the digging of wells , improving sanitary conditions , supplying ‘kambals’ in winter , supply of free educational books and materials , informing the community of social service programmes and financial schemes for the poor taken up by the elected Government , highlightinmg the insurgents atocrities elsewhere , impressing upon them the insurgents concept that he has to influence the population in order to survive , and many other steps/activities which can easily be undertaken by the Army as resources for such activities are not expensive , easily available and can also be supplemented by the local administration.The main point which should be driven home is the population must feel more secure and happy with the presence of the Army and other security forces and should understand that the only objective of the movement is violence and target is the Government , and that they are least bothered about the local community , but consider it therir safe haven where they can hide during the day , where they can get food , shelter and where they can brainwash and recruit people to serve their ends.

One of the oft-overlooked consequences of just about are what we call second- and third-order effects. Once we have targeted someone or something we must know how this has influenced the local population , the insurgent network and even other criminal enterprises in the AO. Second and third order effects which might emerge are:

- We might lose local cooperation.
- We might gain local cooperation.

More enemies may result if the kinetic attack results in vengeance. Going a step further , the removal of the insurgent/s may effect certain civilians (apparent by antagonistic actions , disappearance from their residence apparently to join the insurgents).Which means we can now zero in on them as suspects.

Another difference exists between conventional battles and COIN ops.In conventional battles we detect , identify , get the precise location and then nominate as a target , be it a high value target or a high payoff target.Now Counterintelligence activities ofcourse happen during conventional warfare but not as offensively as in a limited war against insurgents in a limited AO.What I mean to say is it can be one or several of our agents have infiltrated the network or trhat we have penetrated trhe network by turning one or few insurgents to work for us.Now in the same AO it could well be that a company platoon is engaged in ops against the enemy in the Eastern part of the AO.Now if this platoon is not aware of the agents (infiltratrors) in the enemy who might be selected for targeting by our platoon intelligence section , then this is a grave error.Or say we could be using a rouge insurgent unit (turned) who are up against the insurgents and they could equally well do the same thing—target our agents.Hence the number one priority is deconfliction. The targeting cell generates intelligence requirements which the HUMINT collection cell satisfies by its collection operations.Now the two cases cited above or even in a case where our soldiers are fighting behind enemy lines (in the case of COIN we can roughly define that as deep into their territory , say the insurgents dominated Assam jungles) , the platoon may not be able to access the HUMINT cell for information or the current targeting list and then it will autonomously choose and finish off the target—who can very well be one of our own agents. So how do our units avoid targeting our own agents that have been infiltrated within adversarial organizations? WE NEED TO HAVE A CENTRAL AUTHORITY , AN INTELLIGENCE UNIT , WHOSE SOLE RESPONSIBILITY WILL BE TO DECONFLICT TARGETING CELL AND HUMINT CELL ASSETS.This is very important as in most insurgencies , we have to resort to infiltration.We must remember an agent placed in the network is worth 50 machine guns.We cannot afford to lose him due to lack of deconfliction.We then suffer a

counterintelligence defeat in the hands of our very own units.

There is a great difference between intelligence driven targeting and targeting based on surveillance and reconnaissance.Intelligence is crucial.If it is not present integrally in the targeting process , you can not remove the targets efficiently.The success rate will be incredibly low.Intelligence drives the fight.It is required to detect , identify , locate the target precisely , gauge beforehand what can be the second and third order effects , aid in creating target folders as per category , aid in target reduction – in short it is CRUCIALLY IMPORTANT.And Mind you , counterintelligence should go hand in hand as it protects this very same intelligence cycle , vetting the sources , determining if they are genuine , or planted.It helps in knowing and locating important targets of the enemy.It is crucial in in telligence planning.It generates positive intelligence.It is not exactly an intelligence discipline but it is more than that—it is an intelligence and force enabler.In COIN it is indispensable.Its offensive techniques like penetration or infiltration can literraly destroy the center of gravity of the enemy.

In any COIN mission , or operation , just launching an attack (kinetic that is) on the enemy using military commonsense or standard combat tactics and techniques/procedures will not be sufficient.Yes here also you are targeting , but this targeting is the usual destruction/removal of adversial elements in the course of combat as per standard doctrine.You ned to have ‘’targeting ability’’ , not just manage a team of trigger pullers.And the management of these ‘’trigger pullers’’ , the Company or Bn must have the ‘’intelligence element’’ as its brain.Then only you have the required targeting ability so critical for success in COIN.Be it kinetic or personality targeting or non-kinetic or psychological targeting.

The parallel war –that is the control of the local population by both the insurgents and the Army is essentially Information Warfare.That includes propaganda and PSYOPS.I must drive home the most important point in COIN—THE LOCAL COMMUNITY /POPULATION IS THE BEST ASSET OF THE INSURGENTS AND OUR GREATEST THREAT IN TERMS OF COUNTERINTELLIGENCE.This is the ‘human terrain’ distinct from the physical terrain (or developed infrastructure terrain , that is the security forces configure existing buildings etc so as to provide force protection and also building attack resistant/delaying structures) which is usually scanned /surveilled and reconnoitered for intelligence preparation of the battlefield.Ignoring this human terrain , not developing it and utilizing it to our advantage places all gains from intelligence preparation of the battlefield considering the physical terrain , the enemy , the weather and environment to a minimum.We must consider non-kinetic targeting with the same importance like kinetic targeting.We need to maniupulate the minds of the population.They are the ones who can provide us hard much needed information.If we lose their support , the insurgents get their support.

Take a case in point.An army platoon is engaged in a combat action with a group of insurgents and things go wrong.The platoon was initially firmly emplaced in a built up area , protected and hardened against enemy fires.But a prolonged combat resulted in rapid depletion of ammunition and now the soldiers must flee as reinforcements will take long to reach the area.Fine—they did just that.The Company Commander had always recognized the need to influence the human terrain and today this platoon got saved just because of their Commanders foresight.How? On escaping they took refuge among the local population who gave them shelter , hiding them from the enemy , and also intelligence about enemy movements (they are nbow on the lookout for the platoon) both to the soldiers and team leader and also to the headquarters by dispatching a couple of villagers.So they are now the teams cover , intelligence collectors and also supply points.Thats the benefit of information operations in COIN. If you can win the battle for CONTROL , then you’ll make the battle of attrition much more difficult FOR THE ENEMY.Period.

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 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. 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 bottomup 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.

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.

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.

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 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 proinsurgency 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.

PUSHING DOWN INT CAPABILITY

May 6th, 2017

TACTICAL MILITARY INTELLIGENCE CAPABILITY

PUSHING INT CAPABILITY TO BOOT LEVEL

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 ofinterest.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 bottomup 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 lotofinformation 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.

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.

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 situational 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 gathered.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 nonkinetic 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 theenemy.
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.

FORCE PROTECTION

May 6th, 2017

FORCE PROTECTION--AVOIDING URI TYPE ATTACK

Intelligence has two objectives:

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

The second intelligence objective is that it assists in protecting friendly forces through counterintelligence. Counterintelligence includes both active and passive measures intended to deny the enemy valuable information about the friendly situation. Counterintelligence also includes activities related to countering hostile espionage, subversion, and terrorism. Counterintelligence directly supports force protection operations by helping the commander deny intelligence to the enemy and plan appropriate security measures. Stated differently it acts as an early warning system by attempting to provide accurate and timely information about the adversary's intention, and the surrounding environment. It also provides a counterintelligence tool to deny the adversary valuable information and also to combat terrorism, subversion and espionage. Thus intelligence is protective, exploitative and positive in that it supplies us with positive intelligence about the adversary and protects our own infrastructure. Intelligence thus renders our actions either offensive or defensive.

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

Today's war scenario is of the 4th Generation type. Asymmetry has factored in most battle or tactical operations to a great deal. In fact most of the conflicts around the Globe are asymmetrical in nature , with the players in the combat environment being terrorists, insurgents with very limited firepower , elusive and most of the time operating while mobile , very less identifiable with no conventional forces insignia , very limited personnel strength , distributed and sporadic operational tactics, undefined infrastructure logistical capabilities on one hand and a national power or allies with a formidable military, attack and defense platforms and a central military organization with subordinate headquarters and units spread at unique identifiable geographic locations. Hence not to be subdued by this disparity between themselves and govt. forces the asymmetric adversary resorts to sudden, sporadic, hit and run type attacks on the forces bases , installations , camps , ordnance depots, communication systems, personnel and information systems with the sole objective to degrade the forces combat capability and kinetic termination of its key leaders at top echelons or middle and ground level tactical units. A kill is a kill. A kinetic hit is a kinetic hit. Whether it's a bazooka attack destroying an armored personnel carriers drive system immobilizing it or whether it's a timed explosion resulting in the destruction of a combat helicopter in the hangar , the end result is the same….we have lost combat capability. In this fashion attacks on our installations,camps,bases,personnel and information systems/communications are designed to degrade our capabilities, exhaust our ordnance on nonexistent targets or dummy targets / proxy targets (deceptive measures of the adversary) –this realm of Threat to our forces itself while in transit or before deployment or in personnel stations and bases and the Govt. forces actions to thwart these threats with intelligence feeds predicating the plans/ COAs design is called Force Protection.

CI supports Command Force Protection efforts by:

·Identifying the potential threat forces and multidisciplinary threat intelligence

·Identifying threat capabilities and intent together with the most likely course of action and the most dangerous course of action (keeping all the possible COAs parallel for review)

·Using deception to mislead the enemy about our capabilities, vulnerabilities and intentions.

CI & SECURITY REQUIREMENTS:

·Protecting classified information

·Protecting critical resources

·Protecting weapons and weaponry systems

·Safeguarding visitors to the installation

·Protecting dignitaries

·Protecting Senior government officials or military senior stafdf visiting the installation or areas outside the installation but falling within military jurisdiction

·Sustain mission objectives

·Protect information systems

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

Local threat assessment usually provides a threat picture specific to a single installation or grouping of installations based on the threat factors mentioned

above. This means that each installation may have specific security requirements tailored to its individual assessment.

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

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

CI/HUMINT Support to Force Protection: Whether conducting liaison, a Threat/ Vulnerability Assessment (TVA), or a HUMINT collection operation, the focal point for most CI/HUMINT operations is providing support to Force Protection. There are three critical pieces to this support mission on which we focus:

a. Know the Threat: The development of a MDCI Estimate is critical prior to any deployment. Once contingency areas are identified, the HUMINT Single Source Cell within the Control HQ begins developing and maintaining these products. As the Battalion operational plan develops, HUMINT operation management teams aid HUMINT Single Source in gathering information on the AO. The turf is broken down and CI/HUMINT teams work to become subject matter experts on the customs, culture, government, and geography of their given areas. Once in the contingency area, conducting liaison is always the first step. Without the initial preparation to gain knowledge of the area, the team would be incapable of "hitting the ground running" and making the initial liaison contacts required to quickly assess the threat to the force. We look to identify and maintain contact with local police, intelligence, and security agencies; Private Volunteer Organizations (PVO) and Non-Governmental Organizations (NGO); and allied counterparts. Through this liaison the development of CI Force Protection Source Operations (CFSO) occurs. CFSO operations provide Indications and Warnings (I&W) of potential threats to our Forces.

b. Know your Vulnerabilities: Once the threat has been established, the CI/HUMINT teams move their focus toward conducting Threat/Vulnerability Assessments (TVA) on critical army assets and potential enemy targets. The identification of friendly critical assets is derived from determining what the Army Commander considers as his centers of gravity and those assets that compose and support it. Some traditional critical assets include C^3 nodes, logistics sites, aviation and ADA assets, and counterfire radars. The TVA analyzes all the aspects of physical security, personnel security, information security, and communications security. The TVA measures the current threat capabilities against emplaced security measures and operating procedures to identify vulnerabilities. Again, without the previous research in identifying the threat and in conducting liaison, the team would be incapable of making a valid identification of vulnerabilities.

c. Provide Countermeasures: Providing valid countermeasures is often a difficult task to strike the right balance of security with the given assets and environment. Too restrictive of security measures rapidly degrades operational sustainment and builds distrust in the people we are trying to protect as we continue

to throw barriers between us and them. Too lax of security measures provides the enemy with his target of opportunity and forces the Army to pay for a costly mistake in the loss of lives, material, and status in the world's eye. Providing predictive intelligence coupled with valid countermeasures is the apex of CI/HUMINT support to force protection. One tool that we can use with good success in providing predictive intelligence is the 24-hour time-event chart. The 24-hour time-event chart graphically depicts incident reporting on a 24-hour clock chart. Over the span of a couple days, the chart displays the enemy's operational patterns. From this pattern, the analyst can determine enemy sleep cycles, movement, and attack times, aiding the analyst in predicting enemy activities over the next 24 hours. Countermeasures can then be applied to avoid enemy contact on unfavorable grounds and increase defense measures during most likely times of enemy attacks.

DISTINCTION BETWEEN CI AND HUMINT:

CI Does Not Equal HUMINT

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

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

CI on the other hand uses human sources too as source of information but goes few steps further in that CI is aware of the intent of collection and aggressively uses specific techniques to either neutralize or exploit the enemy intelligence activities using the gathered information. Most of the techniques in his repository are similar to that of the HUMINT agent; It is this use of HUMINT skills, particularly investigation and source operations that has created the confusion. CI is a multidiscipline function with the purpose to detect,identify,deter,exploit.neutralize the enemy's collection efforts—itseeks to counter enemy intelligence geared towards terrorist,subversive,espionage,sabotage or insurgent attacks on our forces and installations and lend support to HUMINT in its activities, protect the intelligence cycle and ensure force protection —a very important factor. Thus we find CI to be composed of several attributes,aggressive,never relenting and protecting the other intelligence disciplines activities(for example , determining whether a source

is a source who wants to wittingly give information \or is an enemy plant).HUMINT contributes to an all-source visualization of the battlefield , increases the situational awareness of the commander.HUMINT is intelligence derived from persons,documents,a pure intelligence activity whereas CI is somewhat like the hand in darkness..exploring,detecting,getting a hold. Moving ahead with all help that is available in an unknown enemy specific darkness , the enemy lurking in the shadows , whose actions once discerned by the hand will lead to the latter's firm clasp on his neck.

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

Conclusion

HUMINT collection and CI are and will continue to become increasingly important as we enter the 21st century. Both efforts are vital to mission success across the entire spectrum of operations. The understanding of the doctrinal distinction between HUMINT collection and CI is fundamental. This distinction drives the doctrinal description of both efforts and our understanding of how they are mutuallysupportive and intertwined in stability operations and support operations.Whatever be the divisions in function or overall structure, HUMINT and CI are indispensable to thwart enemy intelligence activities, to conduct force protection in a optimum manner, to keep our forcescombat-ready to deliver precision strikes and to always keep the decision advantage in our favor with the element of surprise by the enemy being put at the minimum. Both disciplines are time intensive and inter-human interactions over prolonged periods have turned the tradecraft into a very specialized skill involving human perception, behavior, psychology and other traits. Unlike other disciplines like SIGINT,IMINT,MASINT,GEOINT HUMINT and CI have in common human sources , the human element and hence is susceptible to error , deception by the enemy , fraught with risks and psychological stress including human vices predicated by money and other factors which are usually the byproduct of information-transactions (quid-pro-quo).But it is exactly these problems which prompts intelligence professionals to come up with newer tactics so as to minimize these negative factors and the resulting exploration and research in the field of HUMINT and CI leads to refined methodologies , TTPs which have been found to be effective in many cases.

Improving Army CI Doctrine

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

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

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

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

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

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

The commanders battlefield operating system at his disposal are fire support and maneuver and here is where intelligence and counterintelligence act as force multipliers –the Intelligence and CI BOS must be successfully integrated in the Commanders BOS so that his PIRs are successfully answered giving

him ideally a perfect situational awareness about the battlespace so as to conduct operations successfully. The commander focuses on the intelligence system by clearly designating his priority intelligence requirements (PIR), targeting requirements and priorities. Intelligence is a continuous process which keeps IEW operations tied to the commander's critical decisions and concept of operations. CI collection, analysis, and dissemination, like other intelligence, have to meet the commander's time requirements to be of any use other than historical.

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

·Enemy units

·Terrorist groups

·Insurgent groups

·Enemy special forces

·Criminal enterprises

·Cybercriminals

·Radical elements

·That part of the local populace which supports the enemys ideals

·Environmental/chemical/health/radiological/biological hazards of the enemy units,terrorists,insurgents and crimninal enterprises

·Weaponry systems

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

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

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

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

ØHUMINT was not given priority in force protection efforts , neither the HUMINT support was adequate

effective and tailored to the Commanders needs. Instead standard operating procedures detailing standard and routine defensive methods and access control were implemented.HUMINTs capability in predicting on how , where and when a terrorist attack might take place was ignored.HUMINT can predict the specific target ,time and nature of attacks.

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

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

ØThe installation in question fell prey to terrorist attacks because the intelligence arrangement at Command level in higher headquarters or at the installation headquarters itself was focused on outward attacks like tactical missions, or defensive postures dictated by air threat and totally ignored the need for HUMINT/CI based intelligence collection for ground defense of the installation, personnel, information and communication facilities.

To execute a CI operation successfully liaison is needed with other civil agencies and with the intelligence agencies of the 3 services.To effectively build up a liaison time is required,it cannot be achieved overnight.In case of COIN operations liaison is much needed with the local administrations intelligence branch and

with the police as they are the ones who know the local area,population,criminal elements and insurgency profile in terms of attack history, police records of personalities and elements who have been apprehended and surrendered..the latter can be put to use by the counterinsurgents as pseudo-insurgents to penetrate the adversary's setup. Liaison relationships are an investment in the future, and the return on this investment is directly proportional to the time and effort expended on developing and maintaining the relationship.

We can transfer say 2-3% personnel from the MI to the CI unit as CI units are generally understaffed compared to the standard HUMINT units , and the liaison units. Even transferring 3% personnel can significantly raise the strength of all the units overall. Thus with this transfer the Commands HUMINT assets get a boost and now coupled with CI augmentation the HUMINT teams can handle all three types of threats , Basic , Levels 1&2.
Simply transferring will not suffice, proper training in counterintelligence need to be given. But this wont be a problem as the MI soldier already has basic intelligence training and acumen. Yes they need to be granted clearance to access compartmentalized intelligence information and hence prior to transfer the soldiers need to undergo a counterintelligence investigation process as to their suitability.

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

What Are We Protecting?

In protecting an installation and its information systems, operations and general security from enemy multidisciplinary intelligence threat we must identify the vulnerable and critical areas to be given more weightage during security review. Not all assets and activities warrant the same level of protection. To this end a careful and thorough vulnerability analysis needs to be conducted resorting to red teaming methodology.
It should be noted at this juncture that it is always the attempts of the enemy intelligence service to subvert our knowledgeable personnel. In a military production unit , say ordnance factory , the senior engineers and quality control scientists have access to sensitive designs and information related to weaponry systems. Similarly classified and top secret documents/information are in the hands of cleared senior personnel. These people are often the target of aggressive enemy counterintelligence agents.

The five basic categories include the following:

1.People

2.Military personnel

3.Activities/Operations

4.Intelligence collection/analysis

5.Sensitive movement of operations/personnel

6.Conduct of sensitive training

7.Communications/networking

8.RDT&E and sensitive technology

9.Production of sensitive technology

10.Protection of nuclear/chemical/biological materials

11.Protection of weapons, explosives, and equipment

12.Information

13.Classified

14.Sensitive Compartmented Information

15.Top Secret

16.Secret

17.Confidential

18.Unclassified

19.System designs

20.System capabilities/vulnerabilities

21.Sensitive methods

22.Facilities

23.Headquarters

24.Field offices/administrative buildings

25.Training facilities

26.Storage facilities

27.Production facilities

28.R&D laboratories

29.Power plants

30.Parking facilities

31.Aircraft hangars

32.Residences

33.Equipment/Materials

34.Transportation equipment/vehicles

35.Maintenance equipment

36.Operational equipment

37.Communications equipment

38.Security equipment

39.Weapons

40.Automated information systems equipment

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

UNIT PROTECTION:

We will define unit not be size or specific function but by any military group capable of offensive, defensive or stability operations.

Unit protection is the process through which combatant and noncombatant personnel, physical assets and information are protected from adversarial threats including adversarial multidisciplinary intelligence threats.Multi layered, active/passive, lethal/non-

lethal offensive and defensive measures are adopted for this purpose. Protection is composed of a variety of active and passive measures (for example, weapons, pre-emption, and warning) in the air, land, sea, and space domains. The goal of unit protection is preventing attacks on the three unit resources , manpower, physical assets and information so that the capability of the unit to maintain its fighting potential without any degradation by the enemy is constantly maintained.

The Army must:

ØDetect the threat

ØAsses the threat capability to degrade the units combat capabilities

ØDecide on protective measures , whether offensive or defensive

ØAct to implement these protective measures

ØRecover in very less time from any damage inflicted by the adversary so that technical countermeasures and tactical procedures may be employed so as to bring back the unit to full operational status in the least time possible.

In order for unit protection to be 100% effective we need to ensure that the following are taken into prioritized consideration by the unit commander:

v*Persistent surveillance*

v*Actionable intelligence*

v*Precise target recognition*

v*Interrogation*

v*Commanders situational awareness*

v*Accurate identification of unit security related intelligence gaps The above factors are contained in the Detect-Assess-Decide system."(DAD).*

In addition unit Command and Control must be properly defined as C2 aids the Commander to take proper decisions in the light of what needs to be done exactly to protect the unit and ensure that this is carried out efficiently.

Protection: Protection is a function which should be given a holistic treatment. Protection should not separately focus on weapons deployment , pre-emption and warning. All three must be integrated. No one is a separate entity. Protection must be proactive. In fact unit protection should never always be passive but must also include active measures.Intellighence , counterintelligence and an admixture of military and cross government capabilities should be employed to the full. Installation/camp protection should look beyond the perimeters. Just employing passive measures(check posts, access control, perimeter security , guard functions , lighting) and OPSEC isn't sufficient. Surveillance teams , counterintelligence operatives should foray outside into adjoining areas , even areas of interest located far from the unit , and the communities in these areas so as to gain information/intelligence and counter enemy reconnaissance/HUMINT/subversive / sabotage/terrorist activities. Counterintelligence should be employed to screen contract workers and suppliers. A counterintelligence review should be conducted periodically on unit personnel. Red teaming should be

taken up by the commander and his staff to ascertain unit vulnerabilities and critical areas.

Add to Detect , Assess and Decide the functions Act and Recover and we have the foundation for a complete protection system on which to base our decisions regarding collection of intelligence , fortifying and strengthening/hardening our bases, decide on the optimum courses of actions , employ forces optimally to act on these decisions and in case of an attack which could not be prevented , recover in the shortest possible time without the base collapsing totally during/after the attack using redundancy measures/backups and thorough protection of critical assets. We should also remember protection has yet another dimension. The enemy might know the protective measures we have employed using intelligence and might attempt to block /prevent/deter our post-attack or pre-emptiveactions , hence protection must take these into account also.

Protection means ‘’time-critical tactical operations’’ ..not just tactical operations. Protection should be a 360 degrees hemispherical capability , meaning protection from land , air and sea based attacks.

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

Thus it is clear from the above that protection must be proactive , intelligence-led and an integrated approach.

Objectives of unit protection are:

Install a warning system

Intelligence preparation of all areas adjoining the base ,camp , the route along which the troops movement takes place –in fact it must be made mandatory for units intelligence section to keep an updated file on the intelligence preparation of the entire area surrounding the base/troop movement route whether or not there is a perception of threat.IPB should include , among other things

·Protection must be proactive , lethal and nonlethal both.

·*Intelligence is the primary tool in protection*

·Increase active/passive protection measures

·Rapid seizure of initiatives

·Rapid transition to decisive operations

·Rapid decision making capacity as tactical operations in unit protection are ‘’time- critical’’.Damage to our forces in combat on the battlefdield or in case of an assymetrical combat , in hilly/urban/jungle terrain but away from base is different than that of an attack on an unsuspecting troop movement or installation/base itself where an attack means catching us off guard ,

unprepared and things move so fast due to the element of surprise our forces do not have enough time to recover , regroup and counterattack in time to thwart the enemy.The enemy may have critical assets in mind when they attack the installation/camp/base.Thus tactical operations are ‘’time-critical’’.Hence to successfully thwart an attack ,should our defences fail …we must be prepared to execute time critical axctions without falling prey to the shock due to the surprise element.This is more so say in the case of an attack on an unsuspecting convoy or troop column.

·Reducing vulnerability to minimum

·Identifying critical assets , protecting them priority of all unit protection systems

·Understanding that most operations will be in a non-linear unconventional operational environment and hence all intelligence , counterintelligence , surveillance , reconnaissance , target determination and nomination, combat oiperations,passive and active protection measures , red teaming , and recovery options should be seen from this perspective.

·Should understand that a complete 360 degree hemispherical protection system must be installed which must be a thoroughly integrated intelligence and operations function keeping the factors DAD in perspective and the factors which come next , viz..Act , Finish and Recover

The following types of threats should be expected in any future conflict-

·Attacks –air based/heliborne—on logistical systems.

·Critical assets will be targeted with precision munitions.

·Staging areas , critical choke points may be targeted using missiles with medium-range to ballistic capabilities.

·Random attacks so as to be unpredictable , IED attacks , terrorist and insurgent attacks and Special Forces attacks may be conducted with twin objectives or any of them..Viz..Effect destruction/undermine our fighting capability and to force the commander to waste resources , ammunition, and unnecessarily divert forces to protect facilities and personnel which in fact are not threatened.

We must remember we are now facing a fourth generation enemy , who will attempt to put in use every means including confusion and deception to overcome the asymmetry/mismatch by increasing uncertainty and making us more susceptible to the element of surprise. The enemy will resort to continuous , random, and non-decisive engagements. The enemy will randomly and continuously threaten and interdict lines of cooperation’s and communications. They will use camouflage and deception to to reduce weapon engagement rangers and degrade our forces advantages in ‘’stand-off’’engagements. There are two objectives herein—first to confuse us so much that we cannot execute the targeting process correctly , target determnination.identification.nomination becomes very difficult against an elusive enemy employing random attack methods , and secondly frequent loss of contact

with this elusive enemy has more negative consequences than that which would have occurred with a conventional more predictable echeloned enemy.

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

Military intelligence brigades coordinate, manage, and direct intelligence and surveillance; they conduct collection management, all-source intelligence analysis, production; and they disseminate information in support of national, joint, interagency, multi-national, regional combatant command, and Army service component requirements.
Unit protection must integrate the protective attributes of different Army Corps. The capabilities in brief of the Corps are as follows:

·The Air Defense artillery provides protection by acting as a warning system , intercepting threats directed from air in the form of missiles and aerial attacks (heliborne..etc) and also provide locational grid information for otrher supporting forces to target.

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

·Engineer Corps protect our force by contributing to its mobility and countermobility thus heightening its survivability.provides the capabilities of survivability, mobility, and countermobility to the force.

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

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

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

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

Unit Protection Functions

It’s very true that conventional military threats exist and are given priority in intelligence activities but

the existence and threat capabilities of asymmetric , nonconventional threats cannot be undermined. Add to these new emerging threats of this category. At the tactical level it is very important to address this type of threat by determining its identity, leadership, capabilities, tracking its location and gauging its intent. We need to detect the enemy entire range of hostile activity including intelligence collection and counterintelligence activities, use this information to assess its capabilities and intent to arrive at the common operation picture COP which brings to light the

relationship between the terrain,enemy,mission,troops,time and the civil environment thus enabling the commander to enter the enemy's decision cycle, gauge its intent more accurately, deliver warning to force s in the area and develop suitable courses of action. After the asses step is over the commander moves on to the decide function wherein an action is decided upon or any existing action is altered or monitiored.Therafter the act function takes over where the course of action decided upon is implemented by tasking the tactical fighting unit to deliver kinetic.nonkinetic attack on nominated targets or passive protection measures..all with the intent to protect the force. Protecting the force should not entirely be passive in nature, the soldiers need to go out and attack nominated targets so as to deter attacks or fail plans to attack our installations.

ACTIVE MEASURES FOR UNIT PROTECTION:

Active measures will provide at stand-off distances, the capabilities to-

We designate a stand-off area outside the installation/ protected area and take active measures to deny unidentified vehicular or personnel movement in that area

·Just like we have a C2 system with respect to any mission, similarly we need to have a C2 mission with respect to active or passive defensive measures and these need to be integrated with the C2 itself. Such active/ passive measures can be remotely controlled lethal/nonlethal measures.

·As for passive measure steps should be taken to deny unidentified/suspect personnel/vehicles movement inside a restricted area/protected area .Areas within buildings,facilities,structures,airfields,ammunition

depot,etc can be effectively protected by employing unmanned remotely controlled nonlethal systems at standoff distances. Measures should be taken with priority to deter personnel and vehicles from entering a protected military installation again using remotely activated lethal/nonlethal systems. Physical barriers, both active and passive can be employed for this purpose.

·There can be instances of enemy fire directed at critical assets of the installation and hence we need to include modular protection packages, automatic or soldier response teams built up specifically for this purpose. The protection system should be integrated again with the C2 system. It is very important to point out

here that all the passive/active measures success depends on a great deal on intelligence/counterintelligence/liaison apart from the remotely/manned protection system deployment. For example we need intelligence to apprehend any infiltrations in our camp in the form of security or non security civilian contractors. Or we can effectively liaise with the civil police/intelligence agencies to build up a mapping of probable anti-installation criminal forces operating in the area who could attempt to launch sporadic fires or explosive attacks, such attacks being in keeping with the criminal group's affiliation with the enemy. Counterintelligence can help in visualizing our vulnerable areas within the installation and then proceed to identify the critical nodes which if damaged can stop the installation operations altogether. This vulnerability assessment coupled with the threat assessment and supported by sound OPSEC practices can give adequate unit protection.

From the force protection perspective CI and HUMINT functions:

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

·Threat intent

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

·Identify threat C2 nodes

·Identify threat logistic routes

·Identify threat social reach, network, and contacts

·Identify threat affiliates in other criminal networks, enterprises

·Identify threat sympathizers in own area of control

·Identify political/administrative figures that support threat ideology

·Threat attack /defense operations location parameters.

·Gauge potential attack/defense methods of threat.

·Recommend C2 setup to thwart threat attack.

·Estimate with reasonable accuracy the expected time of attack.

·Possible locations of Threat listening post/observation posts

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

·Possible enemy IED techniques, infiltration routes, emplacement

·Gauge IED detonation methods/means

·Gauge IED timings

·Possible routes for IED ex-filtration

·Staging areas

·Safe houses

·Weapons and ammunitions storage locations

·Production facilities for IED and other ammunitions/ explosives.

·Find out what supplementary operations threat may resort to

·Recommending countermeasures to threat IED

·Recommending countermeasures to threat ISR/EW

·Determining threat indirect fire parameters, key indirect fire

.

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

Warning is of two types:

(a)Defensive warn

(b)Enemy warn

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

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

It is very important that warning should be unambiguous, accurate and timely/specific,. In addition to this it should be actionable. Warning can be graduated , meaning the level of warning may assume increasing proportions in keeping with the feedback about the enemy which may indicate that it has ceased its operations/.activities temporarily but is conducting discreet operations/ increased intelligence activity masked in the cloak of acceptance of our warning and cessation of open hostilities.

WARNING SYSTEM:

The warning system must have the following features:

·It should allow for redundancies in our act capability systems.

·It should allow for passive proactive means so as to protect our installations, its critical assets, command and control nodes, thus overall reducing the vulnerability of the installation/.protected area.

·It should provide a system of integrating fires to handle threats and precluding enemy attack on our installation , its C2 and critical assets.

·Provide warning of threat intelligence activities.

·Provide warning of existing threat C2 nodes

·Provide warning of threat capabilities, disposition, strength, order of battle

·Provide warning of threat logistic routes.

·Provide warning of threat sympathizers.,

·Provide warning of threats possible attack COAs

·Provide warning of the defense capability of the threat

·Provide warning of threats peculiar /preferred TTPs/ modus operandi

·Provide warning of threats history

·Provide warning of threat movements

·Provide warning of threat leadership

·Provide warning of threat detachments, cells dispersed in and out of the area of operations.

·Provide warning of Threat attack /defense operations location parameters.

·Provide warning of potential attack/defense methods of threat.

·Provide warning of the expected time of attack.

·Provide warning of possible locations of Threat listening post/observation posts

·Provide warning of possible escape routes of threat forces after an attack or defense scenario

·Provide warning of possible enemy IED techniques, infiltration routes, emplacement

·Provide warning of IED detonation methods/means

·Provide warning of IED timings

·Provide warning of possible routes for IED ex-filtration

·Provide warning of Staging areas

·Provide warning of Safe houses

·Provide warning of weapons and ammunitions storage locations

·Provide warning g of the Production facilities for IED and other ammunitions/explosives.

·Provide warning of supplementary operations threat may resort to

·Provide warning of threat indirect fire parameters, key indirect fire

Future Modular Force leaders must be trained to aggressively manage information and instill trust in the output of decision support tools that automated systems provide. Other major implications include adoption of a lifetime of education paradigm and the creation of knowledge centers configured to support professional leader education. Leader development questions include, but are not limited to-

(1)How do we develop leaders ready to deal with the complexity of the contemporary operating environment, threats, and interagency implications?

(2)How can we develop more adaptive leaders, versatile in UP operations?

(3)How do we provide collaborative, distributed training problem solving and decision aids that empower battle command to support commanders, as well as staffs to advising commanders during planning, preparation, rehearsal, and execution of UP exercises and operations?

(4)How are leaders enabled to know the terrain and weather and appreciate their tactical implications for tactical concealment, employment of weapons, mobility, and seeking positions of advantage?

(5)How are leaders empowered to understand the operational environment as well as, or better than, the threat in order to execute UP detect, assess, and decide functions?

(6)How will units enable leaders to know the enemy, friendly unit locations, and their capabilities?

(7)How will units adapt to emerging UP situations more quickly than an adversary?

UP is not force protection, although the application of protection capabilities will positively affect force protection. By integrating the protection capabilities outlined in this CCP, a commander, and consequently, the

---

TOCs DIVNET & INT-ENABLED NCOs

May 6th, 2017

TACTICAL OPS CENTERS AND NETWORKING.

The Division must maintain an intranet capability wherein all intelligence and operations data,historical , current and projected are maintained in the database.For example,all sensors,humint-sigint-elint-comint-techint-masint deployed in the Brigade area of the Division should be able to channel the information collected to the specific tactical operations center Desk NCO.Each Brigade will have seperate TOCs installed for each/group of (as the case may be depending on manpower availability to staff TOCs)company/ companies of every batallion.The humint team will send reports to the HUMINT Desk NCO.Similarly with the other intelligence collection disciplines/sensors.Now after analysis by the analysis element in the TOC the intelligence information is passed on to the LAN server.Say we have as the TOTAL NORTH EAST battlespace comprising of the disturbed States.Every State is broken down territory/area wise into specific area of ops.Each area of ops is subjected to intelligence collection by the Bn Intelligence organic units,wherein the information as said above is passed on to speciic intelligence sensor based TOC.or it could be one TOC may cater to all sensor types with each Desk NCO allocated to each sensor information receipt channel.Each subset area of operations within the boundaries of each State has as its intelligence and ops database input nodes at the TOCs of the Brigade (each Bn)/Bn group.A group of such TOC nodes are conected to one LAN node.In this manner an entire network of LAN nodes are dispersed in each State.The complete LAN WAN NODE will cater to each State intelligence ops as well as all tactical combat ops(linked to all the TOCs of the State AO.).. This entire system in its totality should be viewed as concentric circles.The outermost ring is the deployed sensors (or as I aim to achieve , organic company level-platoon level intelligence sections--that is boot level sensors);The next ring will be the individual TOCs and the DESK NCOs receipt/ dissemination terminals.The inner ring will be the LAN chain of all the States; each LAN being comprised of all the sub-LANs of that State to which feeds come from all the State TOCs.All feeds from this inner LAN ring will be into the next inner ring - the WAN Network Main Server.In this manner we have overcome the probs of decentralized command and control of intelligence and tactical operations in a nonliner distributed wide battlespace (it is not possible for every tactical unit to push upwards all intelligence and combat operation to higher headquarters in a very wide (State) area of operations , there is an inundation of information at Bde level intelligence section--it cannot manage easily even with intelligence detachments sporead out without the installation of Bn-level TACTICAL OPS CENTERS (and Company level organic intelligence cells created out of a team of non-int occupational speciality personnel--like the infantry soldiers,MP,patrols--trained in basic tactical question-ing,elicitation,observation and surveillance skills.The TOCs bring in an element of control and ease of information push to much lower levels than higher HQs for the tactical units deployed.In each sub-sector of each AO within each sub-region of each State the tactical units find it easy to push information to the locally installed TOC.The group of TOCs in the State can exchange information laterally among themselves and get a clear picture of all activities and trends.This helps to give the Bde Commander a clear common operating picture COP--which means the exact ground situation without being inundated with unnecessary or conflicting or excessive intelligence information.(In my CFET web portal I have detailed the battle-staff functions of each TOC wherein cases like deconfliction , technical control of int/counterint TTPs,updating and management of source network and source registries,requirement,collection assets management and collection management,administrative control,ops management,dissemination--all being handled by NCOs and a JCO with one battle Captain).This TOC network through the Overall LAN system of each State can effectively push/pull information from the main WAN Network.Thus we find that an effective command and control of the entire NE intelligence and tactical combat operations is ensured due to the availability of intelligence and combat information at the boot level (Company level int capability and lower) ,TOC level , State level (LAN System) and the entire Battlespace (NE) Level THROUGH THE MAIN WAN NETWORK(Each Bde Level).All Bde's will have their own network system on similar grounds in their AO with the main linkages to the DIV MAIN INT/OPS DATABASE SERVER.This is what I will call the Div Ops and Intelligence Net (the main WAN System).

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

Roles and Functions of Battle Staff Noncommissioned Officers in the Intelligence Warfighting Domain

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

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

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

TOC/CP has two primary functions:

1.To track Soldiers and equipment during the battle, to assist the leader in the command and control of the unit.• 2.To serve as a data center that processes enemy and friendly information

Intelligence (Intel) Function

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

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

• There should be a proper command intelligence training plan and the Battle staff NCOs should see to it that threat force considerations,intelligence,counterintelligence and force protection are properly integrated in this training plan.This will ensure good intelligence readiness.

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

Intel tasks:

• Recommend priority intelligence requirements (PIR).

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

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

Provide support to indications and warning with respect to operations.

Provide support to Force Protection

Provide intelligence support to battle damage assessment.

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

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

Intel synchronization:

Provide support to ISR synchronization , thus reducing wastage of intelligence assets,proper allocation of assets as per availability and capability—all the while keeping the priority intelligence requirements of the commander in perspective.

• Synchronize intel support to operations and to intelligence, surveillance, and reconnaissance (ISR) integration through close coordination with the commander, chief of staff (COS)/ executive officer (XO), S3, and the other staff members.

• Develop and continuously update list of intel gaps.

• Analyze and track commander's critical information requirements (CCIR), PIR, friendly forces information requirements (FFIR), and information requirements (IRs) to develop generic collection tasks and requests for support from higher and adjacent commands.

• Develop the intel synchronization plan.

Other intel support:

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

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

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

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

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

• Debrief friendly personnel.

• Identify linguist requirements pertaining to intel support.

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

• Coordinate security investigations of local-hire linguists.

Counterintelligence:

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

capability or unable to satisfy the Commanders intelligence requirements.

Support to security programs:

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

TACTICAL OPERATION CENTER

May 6th, 2017

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

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

Regarding the last two he need only understand how R&S is conducted , and all the factors that go into it--predeployment,insertion and the two activities itself(collection)--he needent be proificient in R&S,the intelligence asset (the CI man[or one member of the R&S team trained in TQ,DOCEX] with the R&S team) can look for intelligence/CI information while the R&S team does its own bit.

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

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

matrices and overall common operating picture. He is the frontline information manager. The battle staff NCO and battle captain must work together and understand each Other's roles and responsibilities.

Commanders and Staff concentrate on achieving a streamlined picture of the ensuing battle , in fact at any moment of time the Staff and the Commander should be able to grasp the immediate current situation as simply as possible without the presentation getting inundated with information overflow.This common operating picture viewed explicitly and concretely enables the Commander to take swift decisions in an otherwise fast evolving uncertain battle environment.It is not possible for the Staff to accomplish this by themselves and the standard office personnel who assist them (in the Tactical Ops Center)..what is required that the battle staff from among the JCOs,Senior NCO and NCOs assist the Staff Officers in the respective warfighting functions , viz: intelligence and

CI;maneuver;sustainment;command,control,communication and computers C4;plans;fires;protection;engineer and provost marshall functions.The main objective is to acquire the best situational understanding about the common operating picture within the tactical operations center/command post. . The TOC/CP has two primary functions: • To track Soldiers and equipment during the battle to assist the leader in the command and control of the unit. • To serve as a data center that processes enemy and friendly information.

The role of the battle staff is a critical component to achieve mission success in a counterinsurgency environment. Battle staff noncommissioned officers (NCOs) perform a multitude of vitally important roles and functions in the tactical operations centers and command posts. They are the principal managers of battle tracking, which supports the timely analysis and processing of plans and orders, and they continually adapt these plans and orders to counter the threat.

KESHAV MAZUMDAR
ANTITERRORISM OFFICER
KOLKATA.WB.
mi.intelligence@gmail.com
http://bit.ly/armyxxii

NOTE FROM AUTHOR

May 6th, 2017

This is the first part of a series of ebooks I have prepared in the aftermath of Dantewada attacks.My objective is to present our shortcomings where intelligence as a prime enabler of military operations and force protection is often ignored in its entirety-that is to say we do not realize its full potential from different perspectives , such as pushing intelligence capability to the hands of tactical units--the infantry unit itself having its own organic int cell rather than depending for actionable int from higher HQs ..sometimes flung far away from the actual area of ops.Same goes for force protection where counterintelligence assumes a very very important role.We need to secure our bases,personnel ,C2 before we decide to go offensive.That is to say we go forward full ahead with 100% combat capability.The enemy will do its best to attack us when we are inside our camps , bases to destroy our combat adge.Be it morale , C2,lweaponry systems, personnel , our ops plans , and even our intelligence plans-moves--the enemy will try to effect a destruction and even if we lose one unit of our capability , say a soldier we fall short of a 100% combart capability. In this booklet I have touched on these shortcomings and I have introduced TOCs and the Div NET.

All these will bev elaborated in other booklets of the series.

Keshav Mazumdar Antiterrorism Officer
CPO CRC CMAS ASC ATO
Fellow New Westminster College Canada
Reach Me Here

COMPANY LEVEL INTELLIGENCE CAPABILITY

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