Brief for GOC-in-C Northern Command.

DEFENSIVE CONSIDERATIONS IN COIN

By Keshav Mazumdar

PROTECTION

Protection is the maintaining the effectiveness and survivability of military installations, camps, personnel, equipment, information/communication systems and other facilities located within the area of operations in any COIN mission. In case of COIN the protection concept is different than that of a conventional force protection scenario in that the element of the protection of the local populace/communities inhabiting the AO is also taken into account. Now if this element is granted due protection, is secured from the insurgents psychological ops and transactional overtures(seeking safe houses, staging areas in the local area, taking psuedonames or as family members to deceive the forces against a false or ideologically goaded sense of protection for the community members or any other assumed social benefit not accorded by the government) then in turn the security forces gain allies who will feed intelligence about the enemy and information pertaining to military security thus enhancing the security of
the tactical units and installations itself.

TECHNIQUE CONSIDERATIONS DURING COUNTERINSURGENCIES

Insurgents resort to lethal and nonlethal attacks against groups of soldiers, unit commanders and civilians. Lethal attacks include killing and IED whereas non-lethal attacks are kidnapping and ransom, subversion or psychological/intimidation/threats. To thwart such attacks and deter the enemy the following basic site-protection operations may be included as foundation steps in the overall unit protection program.

Observation Post: An OP is inadequately capable of protecting any vital asset of the unit using combat power but it can observe any enemy visual action and alert combat support immediately. It should be capable of defending itself and must have a communications backup/night vision devices and long range binoculars.

Stationary posts and static bases: Each post/base must take into consideration following factors before being assembled:

- Critical asset dimensions
- Threat severity
- Nearest reserve troops in terms of the time to inform them and the distance.

Keeping these into consideration a detachment/s occupies the post/base, full time and equipped with night vision devices and surveillance equipment. Its a very good idea to include mobile surveillance teams to keep an eye in the area in close proximity of the base perimeter.

Patrols:

a) Foot patrols: Both critical and low priority assets may be covered by foot patrols but usually low priority assets are allocated for protection. Foot patrols are susceptible to ambush and hence patrol timings must be random. This also helps in maintaining the element of surprise. Patrols must be well armed to defend themselves and have the necessary communication facility toi call for support if the need arises. The support team should be locally positioned and not far away.

b) Vehicle patrols: All the above apply equally to vehicle patrols.
c) Aerial patrols: Inaccessible areas can be kept under routine patrolling surveillance. Here they supplement foot and vehicle patrols in that they offer an extension in the coverage area. It can so happen that critical assets are positioned long distances away in terrain unsuitable for foot/vehicular patrolling.

RANDOM ANTITERRORISM MEASURES

It is very likely that the enemy keeps our forces and installation under surveillance. Their priority is to discern the overall security plan. Hence to throw them off track we must introduce a random element whenever possible. This also helps us to spring a surprise on the enemy. The main criterion here is to alter the security posture from time to time thus defeating the enemy's surveillance attempts. The enemy through surveillance attempts to know our possible actions,intent,order of battle,dispositions,etc.True surveillance is not strictly an intelligence activity on the part of the enemy but it is an enabler of intelligence. Hence we should tackle enemy surveillance on a equal footing with our intelligence and counterintelligence efforts.
Just like we use deception in counterintelligence based defensive and offensive activities. Similarly we must use randomness to thwart enemy surveillance efforts.

- Vehicular barriers to route traffic around base.
- Random security patrols
- Floodlights should operate at random times.
- Guard duty shifts must be practiced at random times.
- Changing access time for entry points.
- Access procedures/passwords must be changed at random.
- Searching personnel must be randomized—the method that is.
- Maintaining random observation of surrounding areas utilizing unmanned systems if available/remote systems.

Armor Protection

We can increase the quantum of protection considerably by vehicle and personnel armor. But it must be kept in mind armor weight reduces the mobility of both the vehicle and soldier—in the case of the latter his maneuverability and endurance gets affected adversely..In addition heavy armor wears engine parts of the vehicles. But it is true that insurgent attacks become very much ineffective on armor shielded vehicles and personnel.

Hardening

Hardening is intended to defeat or negate /deter an attack.
Hardening makes it very difficult for insurgents to carry out attacks.
Study the terrain carefully and see to it that natural obstacles can be emplaced to deter the movements of the insurgents. Naturally available materials can be used to protect personnel, equipment and facilities. Physical protection can be effected using sandbags, walls, shields, concrete barriers. Proper selection should be made in keeping with nature of attacks: Blast, indirect/direct fires, heat, and radiation. Electronic warfare demands a different set of materials/systems.

COUNTERINSURGENCY BASES

COIN forces must have a base from which to operate and also project. Bases are secure areas from which the COIN objective is to isolate the insurgents from the support facilities and protect the local populace/communities. The base must be carefully selected, reinforced and rendered fully defendable. Command relationships should be clearly defined. Bases can be of 3 types:

Forward operating bases, Combat outposts, and Patrol bases. The nature of the mission and size of the unit (Company etc) determines the size and location of the base.

FORWARD OPERATING BASES

Sometimes the nature of operations, the terrain, the size of the AO as well as the size of the units necessitate a separate forward placed operating base for the Battalion which itself commands controls, communicates and supports deployed units. It provides intelligence support, sustainment, replenishment and personnel support as well as functions also as staging area. Each area of operation may have one forward base. A forward operating base acts as a secure location for the planners and command staff so as to plan operations, provides security to the local populace and acts as a deterrent for the insurgents nearby by hampering their mobility and subjecting them to an increased threat. We can have both Brigade FOBs and Battalion Fobs. In the case of Bde FOBs they act as rear areas for Bn Companies which are forwardly deployed. FOBs should maintain either secured road/water or air sustainment capability.

COMBAT OUTPOSTS

Observation posts are reinforced with fire power and combat teams and hence take the shape of a combat outpost. They are positioned at strategic points inside insurgent-0dominated areas , are company or platoon sized, possess the ability to conduct combat operations on a limited scale and are in contact with base headquarters as well as horizontally with other combat outposts , in effect networking both horizontally and vertically so as to:

Cut of insurgent logistical lines

Provide security to the local populace in the immediate neighborhood of the COP

Maintain direct contact with the local populace and hence keep an eye on the activities / strangers

These are not possible from remote bases operating from outside insurgent dominated areas. The negative factors in this type of arrangement are increased risk to the soldiers and limited area of operations , nevertheless proper networking among the combat outposts helps greatly in keeping a grip on the insurgency and the kill ratio as well as protecting the populace. It is very important to plan the position of the outpost, the emplacement, complete with secure logistical lines, communication systems and reinforcement capability. Each COP is assigned a sector of the AO.

Outposts may be employed—

- To secure key lines of communication or infrastructure.
- To secure and co-opt the local populace.
- To gather intelligence.
- To assist the government in restoring essential services.
- To force insurgents to operate elsewhere.

Priorities of Work
Certain factors need to be considered while establishing combat outposts.

- The selected area must be free of noncombatants , civilians and the like.
- To hinder the enemy's movement , obstacles to his entry to streets , underground passages,marked
areas in rough/jungle terrain should be emplaced.
- Carefully choose positions to set up weapons to cover likely avenues of approach.
- Clearing fields of fire
- Cover and camnouflage.
- Obstacles/barriers may be integrated with weapons so as to be auto-triggered.
- There should be easy access between positions and the routes must not hinder speed.

PATROL BASES
Patrol bases are secured areas which serve as long period halting points for patrols. They may be permanent or temporary.
1. Sometimes it is important for patrols to remain hidden or halt all operations as information is received that they are liable to be detected.
2. Again detailed study of an area requires long periods of reconnaissance so they need a place to hide,and then later launch recce ops.
3. After long periods of recce operations,the troops get exhausted and hence retire to a patrol base for
food,sleep or rest,weapons/equipment maintenance
4. After detailed reconnaissance the patrol commander needs to sit down with his senior NCOs and
devise future course of action
5. In cases when the patrol is in enemy area after infiltrating the area,in small groups , they set up temporary patrol bases where they can later meet and regroup and make further plans.
6. Finally a patrol base is a good launching pad for consecutive or concurrent operations such as
7. raids,reconnaissance,surveillance and ambush.

TERRAIN
Key terrain factors to consider include the following:
- The terrains may add to defense by virtue of its natural characteristics.Hence conduct a thorough study of the terrain.To enhance its natural defensive characteristics more utilize artificial obstacles/barriers.
- The patrol bases must have all access routes to it , by road or waterways , under control.The same applies for all lines of supply and communication and civilian access.
The best technique for base defense is the perimeter defense.

UNIT PROTECTION:
We will define unit not be size or specific function but by any military group capable of offensive, defensive or stability operations.
Unit protection is the process through which combatant and noncombatant personnel, physical assets and information are protected from adversarial threats including adversarial

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

The Army must:

¬ Detect the threat

¬ Assess the threat capability to degrade the units combat capabilities

¬ Decide on protective measures , whether offensive or defensive

¬ Act to implement these protective measures

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

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

- Persistent surveillance
- Actionable intelligence
- Precise target recognition
- Interrogation
- Commanders situational awareness
- Accurate identification of unit security related intelligence gaps

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

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

Add to Detect , Assess and Decide the functions Act and Recover and we have the foundation for a complete protection system on which toi base our decisions regarding collection of intelligence , fortifying and strengthening/hardening our bases,decide on the optimum courses of actionsd ,

employ forces optimally to act on these decisions and in case of an attack which could not be prevented , recover in the shortest possible time without the base collapsing totally during/after the attack using redundancy measures/backups and thorough protection of critical assets.We should also remember protection has yet another dimension.The enemy might know the porotective measures we have employed using intelligence and might attempt to block /prevent/deter our post-attack or pre-emptive actions , hence protection must take these into account also.
Protection means ‘’time-critical tacrtical operatiuons’’ ..not just tactical operations.Protection should be a 360 degrees hemispherical capabilkity , meaning protection from land , air and sea based attacks.
For protection intelligence is critical as everything needs to be known about the enemy , envirobnment and self.The last factor is determined by counterintelligence vreviews , technical experts and red teaming.DAD abilities must be thoroughlky integrated to handle attacks fro m land , air,information , electronic,CBRNE,and intelligence domains of the enemy.This integrated approach heightens the commanders situational awareness consuiiderably , thus acting as a forc e and decision-superiority enbabler thus leading to optimum effective course odf acrtion/s by the Commander with a decisive finish.

Thus it is clear from the above that protection must be proactive , intelligence-led and an integrated approach.
Objectives of unit protection are:
Install a warning system
Intelligence preparation of all areas adjoining the base ,camp , the route along which the troops movement takes place –in fact it must be made mandatory for units intelligence section to keep an updated file on the intelligence preparation of the entire area surrounding the base/troop movement route whether or not there is
a perception of threat.IPB should include , among other things:

- Protection must be proactive , lethal and nonlethal both.
- Intelligence is the primary tool in protection
- Increase active/passive protection measures
- Rapid seizure of initiatives
- Rapid transition to decisive operations
- Rapid decision making capacity as tactical operations in unit protection are ‘’time-critical’’.Damage to our forces in combat on the battlefdield or in case of an assymetrical combat , in hilly/urban/jungle terrain but away from base is different than that of an attack on an unsuspecting troop movement or installation/base itself where an attack means catching us off guard , unprepared and things move so fast due to the element of surprise our forces do not have enough time to recover , regroup and counterattack in time to thwart the enemy.The enemy may have critical assets in mind when they attack the installation/camp/base.Thus tactical operations are ‘’time-critical’’.Hence to successfully thwart an attack ,should our defences fail …we must be prepared to execute time critical axctions without falling prey to the shock due to the surprise element.This is more so say in the case of an attack on an unsuspecting convoy or troop column.
- Reducing vulnerability to minimum
- Identifying critical assets , protecting them priority of all unit protection systems

• Understanding that most operations will be in a non-linear unconventional operational environment
and hence all intelligence , counterintelligence , surveillance , reconnaissance , target determination
and nomination, combat oiperations,passive and active protection measures , red teaming , and recovery options should be seen from this perspective.
• Should understand that a complete 360 degree hemispherical protection system must be installed
which must be a thoroughly integrated intelligence and operations function keeping the factors

DAD
in perspective and the factors which come next , viz..Act , Finish and Recover
The following types of threats should be expected in any future conflict-
• Attacks –air based/heliborne—on logistical systems.
• Critical assets will be targeted with precision munitions. Staging areas , critical choke points may be targeted using missiles with medium-range to ballistic capabilities.
• Random attacks so as to be unpredictable, IED attacks, terrorist and insurgent attacks and special forces attacks may be conducted with twin objectives or any of them...viz...Effect destruction/undermine our fighting capability and to force the commander to waste resources, ammunition, and unneceesarily divert forces to protect facilities and personnel which in fact are not threatened.
We must remember we are now facing a fourth generation enemy , who will attempt to put in use every means including confusion and deception to overcome the asymmetry/mismatch by increasing uncertainty and making us more susceptible to the element of surprise.The enemy will resort to continuous , random,and non-decisive engagements.The enemy will randomly and continuously threaten and interdict lines of operations and communications.They will use camouflage and deception to to reduce weapon engagement rangers and degrade our forces advantages in ‘’stand-off’’ engagements.There are two objectives herein—
first to confuse us so much that we cannot execute the targeting process correctly , target determnination.identification.nomination becomes very difficult against an elusive enemy employing random attack methods , and secondly frequent loss of contact with this elusive enemy has more negative consequences than that which would have occurred with a conventional more predictable echeloned enemy.

HUMINT and CI are two disciplines which help in detecting enemy capabilities, intent and countering enemy intelligence collection activities. In a typical Army Intelligence structure, the intelligence assets are located at Div and Bde levels , with the Bde having a HQ company and Intelligence Bn , each Bn catering to a specific collection/counterint discipline. For example there can be a Ops Bn , a reconnaissance Bn , a tactical exploitation Bn,a forward collection Bn ,or a strategic SIGINT Bn.There is also a Div MI Bn and a theater intelligence Bde.
Military intelligence brigades coordinate, manage, and direct intelligence and surveillance; they conduct collection management, all-source intelligence analysis, production; and they disseminate information in support of national, joint, interagency, multi-national, regional

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

1. The Air Defense artillery provides protection by acting as a warning system , intercepting threats directed from air in the form of missiles and aerial attacks (heliborne..etc) and also provide locational grid information for otrher supporting forces to target.
2. Military Police provides security by executing proactive intelligence led policing.
3. Engineer Corps protect our force by contributing to its mobility and countermobility thus heightening its survivability.provides the capabilities of survivability, mobility, and countermobility to the force.
4. Military intelligence provides security to our force by adequate synchronized utilization/deployment
   of ISR assets and counterintelligence capability
5. Signals protects our command and control nodes directing/controlling communiucation,computers,and intelligence operations. Siugnals intelligence directly supports
6. HUMINT operations to validate information,increase the situational understanding of the Commander.
7. Field Artillery provides security to the force by contributing to the direct/indirect firepower,predicting impact points.
8. Ordnance Corp contributes to recovery by deploying its ordnance disposal systems.
9. Unit Protection Functions

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

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

CI/HUMINT Functions:
Recommending countermeasures after assessment of threat capabilities, operations, expected courses of
actions, most likely COA and most dangerous COA.
Threat intent
Identify Threat leadership. Key commanders. Key lieutenants and area commanders
Identify threat C2 nodes
Identify threat logistic routes
Identify threat social reach, network, and contacts
Identify threat affiliates in other criminal networks, enterprises
Identify threat sympathizers in own area of control
Identify political/administrative figures that support threat ideology
Threat attack /defense operations location parameters
Gauge potential attack/defense methods of threat.
Recommend C2 setup to thwart threat attack.
Estimate with reasonable accuracy the expected time of attack.
Possible locations of Threat listening post/observation posts
Determine possible escape routes of threat forces after an attack or defense scenario
Possible enemy IED techniques, infiltration routes, emplacement
Gauge IED detonation methods/means
Gauge IED timings
Possible routes for IED ex-filtration
Staging areas
Safe houses
Weapons and ammunitions storage locations
Production facilities for IED and other ammunitions/explosives.
Find out what supplementary operations threat may resort to
Recommending countermeasures to threat IED
Recommending countermeasures to threat ISR/EW
Determining threat indirect fire parameters, key indirect fire

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

(b) Warning is of two types:
- Defensive warn
- Enemy warn

In defensive warn after receiving actionable intelligence about the adversary's possible attack the installations security is beefed up by incorporating protective measures. The warning may be digital/aural/physical or virtual.
In enemy warn the enemy is communicated the fact through non-lethal measures such as interrogation or challenging an enemy unit/capability that in case of persistent or continued enemy action our course of action/s can take on an increasingly lethal nature with the intent to prevent the enemy from taking further hostile actions and also inflict heavy damages. Thus enemy warn is a method to deter the enemy from carrying out its intent if it hasn't done so yet or to stop the enemy in its tracks...
It is very important that warning should be unambiguous, accurate and timely/specific,. In addition to this it should be actionable. Warning can be graduated; meaning the level of warning may assume increasing proportions in keeping with the feedback about the enemy which may indicate that it has ceased its operations/.activities temporarily but is conducting discreet operations/increased intelligence activity masked in the cloak of acceptance of our warning and cessation of open hostilities.

WARNING SYSTEM:
The warning system must have the following features:
1. It should allow for redundancies in our act capability systems.
2. It should allow for passive proactive means so as to protect our installations, its critical assets, command and control nodes, thus overall reducing the vulnerability of the installation/.protected area.
3. It should provide a system of integrating fires to handle threats and precluding enemy attack on our
installation , its C2 and critical assets.
4. Provide warning of threat intelligence activities.
5. Provide warning of existing threat C2 nodes
6. Provide warning of threat capabilities, disposition, strength, order of battle
7. Provide warning of threat logistic routes.
8. Provide warning of threat sympathizers.,
9. Provide warning of threats possible attack COAs
10. Provide warning of the defense capability of the threat
11. Provide warning of threats peculiar /preferred TTPs/modus operandi
12. Provide warning of threats history
13. Provide warning of threat movements
14. Provide warning of threat leadership
15. Provide warning of threat detachments, cells dispersed in and out of the area of operations.
16. Provide warning of Threat attack /defense operations location parameters.
17. Provide warning of potential attack/defense methods of threat.
18. Provide warning of the expected time of attack.
19. Provide warning of possible locations of Threat listening post/observation posts
20. Provide warning of possible escape routes of threat forces after an attack or defense scenario

21. Provide warning of possible enemy IED techniques, infiltration routes, emplacement
22. Provide warning of IED detonation methods/means
23. Provide warning of IED timings
24. Provide warning of possible routes for IED ex-filtration
25. Provide warning of Staging areas
26. Provide warning of Safe houses
27. Provide warning of weapons and ammunitions storage locations
28. Provide warning g of the Production facilities for IED and other ammunitions/explosives.
29. Provide warning of supplementary operations threat may resort to
30. Provide warning of threat indirect fire parameters, key indirect fire

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

- We designate a stand-off area outside the installation/protected area and take active measures to deny unidentified vehicular or personnel movement in that area
- Just like we have a C2 system with respect to any mission, similarly we need to have a C2 mission with respect to active or passive defensive measures and these need to be integrated with the C2 itself. Such active/passive measures can be remotely controlled lethal/non-lethal measures.
- As for passive measure steps should be taken to deny unidentified/suspect personnel/vehicles movement inside a restricted area/protected area .Areas within buildings,facilities,structures,airfields,ammunition depot,etc can be effectively protected by employing unmanned remotely controlled nonlethal systems at standoff distances. Measures should be taken with priority to deter personnel and vehicles from entering a protected military installation again using remotely activated lethal/nonlethal systems. Physical barriers, both active and passive can be employed for this purpose.
- There can be instances of enemy fire directed at critical assets of the installation and hence we need to include modular protection packages, automatic or soldier response teams built up specifically for this purpose. The protection system should be integrated again with the C2 system. It is very important to point out here that all the passive/active measures success depends on a great deal on intelligence/counterintelligence/liaison apart from the remotely/manned protection system deployment. For example we need intelligence to apprehend any infiltrations in our camp in the form of security or non security civilian contractors. Or we can effectively liaise with the civil police/intelligence agencies to build up a mapping of probable anti-installation criminal forces operating in the area who could attempt to launch sporadic fires or explosive attacks, such attacks being in keeping with the criminal group's affiliation with the enemy. Counterintelligence can help in visualizing our vulnerable areas within the installation and then proceed to identify the critical nodes which if damaged can stop the installation operations altogether. This vulnerability assessment coupled with the threat assessment and supported by sound OPSEC practices can give adequate unit protection.

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

(1) How do we develop leaders ready to deal with the complexity of the contemporary operating environment, threats, and interagency implications?
(2) How can we develop more adaptive leaders, versatile in UP operations?
(3) How do we provide collaborative, distributed training problem solving and decision aids that empower battle command to support commanders, as well as staffs to advising commanders during planning,
preparation, rehearsal, and execution of UP exercises and operations?
(4) How are leaders enabled to know the terrain and weather and appreciate their tactical implications for tactical concealment, employment of weapons, mobility, and seeking positions of advantage?
(5) How are leaders empowered to understand the operational environment as well as, or better than,
the threat in order to execute UP detect, assess, and decide functions?
(6) How will units enable leaders to know the enemy, friendly unit locations, and their capabilities?
(7) How will units adapt to emerging UP situations more quickly than an adversary?
Note: UP is not force protection, although the application of protection capabilities will positively
affect force protection. By integrating the protection capabilities outlined in this CCP, a commander,
and consequently, the force will be offered superior protection abilities.
ISR assets require the flexibility to detect a wide range of emerging threats. While the ability to detect conventional military threats remains important, the ability to address the asymmetric, non-conventional threat gains importance. Tracking the location and activity and predicting the intent of individual threats is a new challenge at the tactical echelon. The following are future enhanced capabilities to address the future environment and will aid in the execution of the UP detect function.

KESHAV MAZUMDAR CRC CMAS CAS FNWC ASC CPO ATO