LEVERAGING TECHNOLOGY IN COUNTER INSURGENCY OPERATIONS

Introduction

21st Century is characterised by phenomenal growth of technology specially Information Technology (IT). The technology is becoming cheaper, easy to operate and provide facilities which could not be even imagined decade earlier. Technology is also a great leveller. "With the possible exceptions of night-vision devices, Global Positioning Systems, and shoulder-fired missiles," writes retired Major General Robert Scales, a former commander of the US Army War College, "there is no appreciable technological advantage for an American infantryman when fighting the close battle against even the poorest, most primitive enemy." Technology is available to security forces as well as terrorists. Today's enemies are dynamic, unpredictable, diverse, fluid, networked and

constantly evolving leading to complex problem sets. Small networked organizations like insurgents are very good at adopting technology whereas hierarchical bureaucratic organizations like Army takes its own time to exploit its benefits. Since Counterinsurgency Operations (CI Ops) is fought basically at battalion or below level, we must provide all the technological support at that level. It is up to us to make use of technology in Counter Insurgency Operations (CI Ops).

Preview

For leveraging technology in CI Ops we need to look into the aspects of various technologies specially network technologies, Software Analysis Tools, sensor and weapon related technologies, how intelligence, the most important factor in any CI Ops can be acquired with the presently available technologies, creation of dynamic database in respective area of responsibility and defensive measures. Information Warfare and some cautionary thoughts also have been discussed.

Network Technology.

The term network technology is referred to as command, control, communication, computer, intelligence, surveillance, and reconnaissance (C4ISR) technologies in military parlance, as well as the consumer-oriented technologies that can often provide the functionality needed for terrorist operations. These network technologies can include connectivity technologies (e.g., wireless routers), mobile computing (e.g., laptop computers), personal electronic devices (e.g., personal digital assistants and cell phones), IT services and Internet access and video recording, among others. If the primary goal of security forces is to defeat a terrorist organization in the long run, there may be opportunities to turn the terrorist organization's use of network technology tools to the security force's advantage by exploiting the information that

network technology collects, stores, and transmits to enable attacks, arrests and other direct actions against the terrorist group.

Internet. Although the Internet is not new, improvements in computer, communications and storage technology have made it a medium of choice for networking, information-gathering and anonymous activities by the terrorists. These tactics include instant messaging, chat, bulletin boards and a constantly shifting collection of Web sites where propaganda can be posted. Terrorists have developed sophisticated encryption tools and creative techniques that make the Internet an efficient and relatively secure means of correspondence. These include steganography, a technique used to hide messages in graphic files, and "dead dropping": transmitting information through saved email drafts in an online email account accessible to anyone with the password. Lately, it has been discovered that they have been using porn sites and chat rooms on the Internet for exchanging messages. For instance, in the terrorist strike at Red Fort, militants of the Lashkar-e-Toiba group were found to have used a cyber-cafe in North Delhi as a communication link for the operation. During the investigations, Delhi police was initially taken aback to find nothing except pornographic pictures stored in the computers. Later they realised that the pictures contained hidden encrypted messages. The Internet also provides a global pool of potential recruits and donors. Online terrorist fundraising has become so commonplace that some organizations are able to accept donations via the popular online payment service, PayPal.

The growth in bandwidth combined with development of new software has enabled unsophisticated users to develop and disseminate complex information via the Internet. For example, in December 2004, “a militant Islamic chat room posted a twenty-six minute video clip with instructions on how to assemble a suicide bomb vest, along with a taped demonstration of its use on a model of a bus filled with passengers.” For those seeking a more accessible way to communicate with others who have a similar affinity for terrorism, Google’s Orkut software— a popular, worldwide Internet service—provides a useful tool. Terrorist web forums provide links to several magazines, which outline step-by-step instructions for communicating with cell members, defining tactics and procedures, and constructing explosives, among other topics.

Communications. With the expansion in the area of operations of insurgents and their external networking specially trans border, insurgents are resorting to modern means of communications such as telephones including satellite phones, FAX, cell phones, E-Mail, World Wide Web (WWW) etc.

The ongoing proliferation of modes that use digital technologies enables low-cost encryption that can greatly complicate the job for the security services searching through the messages. Integrated encryption tools and downloadable privacy software that allows users to encrypt personal phone calls, text messages and other communications among their electronic devices are likely to become widely available. The problem for security forces is that a message can take substantial time and resources to decrypt and it is not possible to predict whether the cipher is vulnerable to exploitation or whether the message is valuable. These limitations, plus the substantial public policy issues they raise, imply that encryption can importantly disrupt intercept operations by security forces. Nonetheless, a dedicated code-breaking effort by security services with adequate resources and time can overcome many

forms of encryption. In the end, the encryption's value is that it buys time for the terrorist organization.

Future communication technologies may also provide the ability for seamless and dynamic shifts of communication modes from short-range wireless communication standards (e.g., WiFi, Bluetooth) to conventional wireless cell phone frequencies (e.g., CDMA, global system for mobile communication [GSM]) and back. For security forces monitoring terrorist communication, such mode nimbleness can increase the challenges of successfully using terrorist communication traffic. For instance, a cell phone with only CDMA has only a single mode of communication, but a wireless cell phone with built in WiFi capabilities has two modes. When the device is in range of a WiFi network, the device can be used to make VOIP calls using the wireless connection to the Internet, and when it is out of the range of WiFi networks, it automatically reconfigures itself to use the CDMA cell phone network. Terrorist access to easy-to-use devices with multiple modes of communication present challenges for security forces attempting to intercept or track communications because they must have the equipment and in some cases, the legal authority appropriate for each mode. Since obtaining the proper equipment and authorities can rely on completely different infrastructures, technologies, hardware, and communication protocols, this can be a very complex and expensive undertaking.

Cell Phones. If one wants to know how people are moving and interacting on a day-to-day basis, there is no information quite as rich as what the cell phone system routinely collects by the minute. Every time someone makes a phone call, some switch, in the normal course of doing its job, records who is calling, where the caller is, who is being called, where the called party is and how long the call lasted—that is, the *externals* of the phone call. Everything important about a cell phone system stems from its software—what goes into the handset and, more importantly, what goes into the switch (e.g., that determine which calls are route, or which information is retained). To ensure real-time collection, security and proper distribution, government should control this software, either by inserting modules into the code base or developing specifications for the cell phone owner to the same effect. If the cell phone system, however, is not architected to deliver such information it will be of no use to security forces.

Militants attempt to avoid signal intelligence technologies. For example, cell phones are given to friends or cousins to organize missions. Callers are instructed to keep conversations to a minimum and to use code words. Additionally, militants change their phones, limiting calls as much as possible immediately prior to operations. They have taken specific actions to further diminish members' cell phone use for attack coordination by prohibiting using cell phones during operations. Recently Talibans have attacked cell phone towers in Afghanistan fearing that all their conversations are being intercepted by US intelligence agencies.

A solid reliable cell phone infrastructure can also permit cell phones to be used as the *primary* communications device of security forces. The problem of interoperability of means of communications between Army, BSF/CRPF and State police forces will be` drastically reduced. Also, some high-end cell phones should be made available equipped with the Scientific Analysis Group(SAG) approved secrecy device. Till such time these are procured commercially available low grade secrecy devices like scramblers can be used

Intelligence

Intelligence is the most important factor in any CI/CT Ops. Technology can be very effectively used for getting actionable intelligence.Some of the tools are explained below.

Software Analysis Tools for Intelligence Analysis. "Part of the problem is that the intelligence staffs are so much under time pressure to show things to senior officers that they present information but not analysis. They don't have time to do analysis. Now we have hours and not weeks or months and that needs to be fixed." Huge amounts of historical and present data and inputs in various forms like satellite photo, UAVs, video and communication intercepts and inputs from intelligence agencies are available. However, analysis of the data and converting into actionable intelligence in the formation headquarters is a critical issue for Intelligence Staff. Trends Analysis and activity pattern can be made. Understanding the mind set, capabilities and intentions of groups potentially operating in specific areas through the analysis of particular groups ideological objective, group dynamics, modus operandi and capabilities can aid analyst in better assessing how the group is likely to operate in or threaten a particular region. Intelligence inputs are required to be quantified and identified in somewhat discrete form to be used for comparison and trend analysis. Normal behaviors when filtered out, will leave indication of abnormal behaviour the commander can chose to watch, intervene or leave as the case may be. An example of how information about an insurgent group can be analysed for generation of comparison and trend analysis is given at Appendix A.

Association matrixes, network analysis, cultural analysis, genealogy, event-pattern analysis, language-pattern analysis, traffic-flow analysis and financial transaction analysis are tools that should be staples of the intelligence effort in a counterinsurgency. Ambushes, raids, IED and mortar attacks, sniping attacks, and other terrorist actions are complex serial crimes. Property ownership and mapping, a valuable tool in counterinsurgency, can identify community power brokers, vested interests and family connections. Financial transactions, cell phone transmissions and travel patterns can provide valuable data to intelligence analysts. Finding the terrorist is a function of detective work. Who is he? Who does he work with? Who are members of his family, and where do they live? What is his background? Who are his associates? Extensive data files are a boring but necessary part of finding the terrorist. However, computer data mining can ease the job considerably by providing assistance in incident analysis, optimum force deployment, risk assessment, behavioural analysis, DNA analysis, force and infrastructure protection

Computer software can be very effectively used for analysis of vast data. We are software capital of whole world. Developing such a software is no big deal. The problem is, most of the software developers have no previous knowledge of Army. They have to be explained what do we want, in what format and what are the inputs available. Unfortunately staff is invariably busy handling daily issues and briefings, adequate time and attention to these software personnel are not given and we don't get what we want. Unless we sit down with the professionals for long hours, interact with them intimately, understand each other's point of view useful software cannot be developed.

To train analysts to work with such software and modern investigative techniques is a separate issue. Analysts require training in information gathering, data mining, data development, case management, link flow event analysis, detecting hidden assets, post

seizure analysis, matrix development, chart development, pattern analysis, alternative competing hypotheses, and communications analysis.

Intelligence Preparation of the Area of Responsibility(IPA). In any conventional war we carry out Intelligence Preparation of the Battlefield (IPB). Similarly for CI Ops IPA is required to be carried out. Tools available with CI Forces are satellite imagery, google maps/wikimapia, conventional maps, photographs taken from helicopter mounted cameras, UAV, digital cameras, census data, data obtained by soldiers on the ground etc. CI Forces like Rashtriya Rifles(RR) formations and units are located more or less in the same areas. The database` of the area of responsibility including demographic details, details of terrain, photographs of personnel, ID card, habitats with special emphasis on terrorists and their sympathizers and so on should be made. The same database would be useful for WHAM activities. This database should be continuously updated.

Northern Command, in the forefront of CI/CT Operations of the country has taken a quantum leap recently in making IPA. Smart IT savvy officers from staff and signals with their ingenuity, innovation and resourcefulness have juxtaposed satellite imagery, google maps, conventional maps, UAV / helicopter mounted cameras and digital cameras with demographic database and Geographical Information Systems (GIS) software to arrive at a workable solution to meet today's requirements. Though not a perfect solution by any chance, but it is an effective precursor to things that can happen. Very wisely, army hierarchy did not try to centralise the efforts, "let the hundred flowers bloom" and took a bottoms up approach. The CI Forces today have an effective IPA to work on. Linking of databases, standardization of GIS packages or their interoperability, making them web enabled, security features for accessing the databases etc should be subsequently undertaken centrally at Army headquarters level. CI Forces carrying out CI/CT Ops in Eastern Command like Assam Rifles formation and units should have a look at what has been achieved in Northern Command and make their own IPA suiting the peculiar requirements of Eastern Command.

Map with 3D Model. Today we have maps and images from internet or satellites and video or images from UAVs. Maps are flat, outdated and incomplete. What we require is a three dimensional version of the map. We would like to know where :-

- The buildings are, because they limit our line of sight and provide locations where snipers can wait to kill.
- The roads and alleys are because they provide ways for you to maneuver.
- Barricades and hedges are because they can get us trapped.

Buildings have shapes—complex, three dimensional shapes, not just flat outlines on a map. Windows allow militants to see you; walls don't. Wooden doors can be kicked in; steel doors can't. Bullets penetrate plywood walls, but not brick blocks. The shape and composition of buildings clearly affect the options available, both to us and to the terrorists.

We want as much historical information as possible about the vehicles and people that have moved around in the structures shown on a map. People go to mosques at prayer time. They go to market when the market is open. A meeting at a mosque or market outside normal hours

may be perfectly benign, but it's not part of most normal scripts and, therefore, might influence our course of action. All the normal behaviours, when filtered out, leave indications of abnormal behaviour. Warned of abnormal behavior, we can choose to watch, to intervene, or to leave—but we have the initiative.

But maps do not only supply names; they provide something even richer: relationships. Maps indicate many kinds of spatial relationships—adjacency of buildings, connectivity of roads, traversibility of waterways—all of which are important to urban operations. There's an even richer source of relational information that we must consider: an ordinary telephone book. It gives the address and occupation of people. Soldier can ask pointed, precise questions of people on the street to fill up any gap in our information. Information that's been stitched from images, maps and telephone books into a consistent, up-to-date description of the situation expressed as shapes and materials, track histories, and activity patterns can always be helpful to soldiers in an urban area.

An example in diagrammatic form is given at Appendix B.

In 1993 when various procedures of carrying out CI/CT Ops were not yet formalised a operation was taking place in Baramulla town. The GOC with his Col GS went to the site to personally supervise the operations. Suddenly one of the windows from a nearby house opened and a terrorist started firing with his AK-47 killing the Col GS and the GOC was wounded. The point is that whether the CI Force responsible for Baramulla town today, be it RR or BSF or CRPF, has the information available to them which was the house, who are their present occupants, are they sympathetic to terrorists, are there any underground hide outs in that house etc? This type of database needs to be continuously updated and at the click of a mouse the information should be available.

Satellite Imagery. Today if one logs on to www.maps.google.com in internet one can see his location with good resolution for free. Even the US Armed Forces are denying Google to carry out mapping of their bases. If one pays to satellite agencies it is easy to obtain on line images of a particular place. This can be extremely handy. Brigade Commanders and Battalion Commanders should be able to pay and obtain satellite images directly without any bureaucratic process. CI Ops is time specific. If one has to wait for approval through our very hard nosed bureaucratic process the purpose will be defeated.

UAVs. Unmanned Aerial Vehicles (UAV) should be used most extensively in CI Ops. The number of UAVs with formations directly involved with CI Ops must be increased considerably, infrastructure created and utilized to the maximum. The Israeli government has used AH-64 Apache helicopters as well as unmanned aerial vehicles to monitor electronic communications in the West Bank and Gaza Strip. Hand held smaller version of UAVs like Raven used by US Army in Iraq has paid great dividends. Ravens weigh just four pounds and is used by smaller units or sub units like battalions and companies in Iraq and Afghanistan.

Digital Camera. Enough digital cameras have been made available. More are being procured. These should be extensively used.

Biometric Device. Finger printing, retina identification or voice identification methods should be used to identify any suspected person and the biometric identification can be quickly crosschecked with existing data bank for identifying him. The Ministry of Defence should

recognize that collection of biometric identification is a basic war fighting capability, especially when fighting terrorists who hide among the civilian population. These devices should be available at the edges where there is action.

When a terrorist is captured in the field, it is important to "freeze" the terrorist's identity so that he can always be identified as an enemy and a potential threat. False names, passports and nationalities cannot mask the data found in fingerprints or DNA. New technology allows security forces to verify Identity cards with biometric devices that scan hands and faces. Over the period of time the population is getting electronically mapped by voter Identity Cards, Ration Cards, PAN Cards, Bank account numbers, Passport Cards, Driving Licenses etc. With modern data mining techniques and use of biometric devices it would be possible to link up various details of any individual. A start is required to be made specially in states like J and K and certain states of North Eastern India.

Aerial Photo Reccee and Video Photography.

Role of Air Force. Though the Royal Air Force had been using airpower in North West Frontier Province from 1919 till 1947 with great success it is quite surprising that Indian Air Force (IAF) has hardly any role in CI Operations where a very large part of Indian Army is permanently deployed. There are only couple of known cases of use of air power in CI Ops. Once in February 1966 when Mizo National Front armed rebels surrounded a company sized Assam Rifles post in Aizawl, 61 Mountain Brigade with IAF support managed to break the siege. In early 2003 and mid 2004 helicopter gunships were used in Hilkaka and Doda in J &K. In all the cases operations were outstanding success.

Air forces can contribute significantly to counterinsurgency campaigns. In addition to surgical strikes against terrorists/insurgents using precision weapons with exact intelligence, airpower should contribute significantly to the campaign by providing constructive effects through information operations, airlift, aeromedical evacuation, other forms of assistance and most importantly ISR. Airpower provides ISR capabilities that can help locate, identify and track insurgent forces—services that reside in no other service component. Air and space platforms must be tailored to match the unconventional and small scale of the counterinsurgency effort. UAV and satellite imagery should be suitably integrated. Excellent Photo Reconnaissance (PR) resources are available with IAF as one of the main tasks of any AF is PR. How do we exploit this tremendous resource for CI Ops? Fast moving Jaguars and such other aircrafts of its ilk have problems due to their requirement of moving at a particular height and speed. The mountainous terrain the folds on ground and the dense jungles prevalent in our Area of Operations of CI Ops do not give the result we require. If the task is given to IAF, they would certainly come out with bright ideas with their technical expertise, ingenuity and innovativeness. Smart, innovative and thinking commanders have utilized slow moving AN-32 aircrafts flying low with reduced speed with their tails open and video photographed in specific location, got unexpected good results and could even neutralise NSCN (IM) main camp in mid 90s. Infrared (IR) scan also were tried but could yield very little. Hot spots identified when investigated were found to be fires used by wood cutters/ wood maphia or shepherds/nomads. No wonder Americans are trying to revoke already discarded slow moving aircrafts used in Vietnam for photography missions.

However, the Air Force is extremely hesitant to associate itself directly in counter terrorist operations for fear that its assets would be targeted by terrorists. One is tempted to ask what

is the use of the helicopter gunships and the attack helicopters if at the hint of use of any manportable air defense missiles (MANPADS) the air force refuses to fly them as was evident in Kargil conflict. Surely in conventional war enemy anti aircraft weapons density would be far more. When the same aircrafts were used very effectively by Russians in couple of hundred kilometers away from Kargil at Afghanistan in early 80s where were the flares and accompanying technology and tactical flying? We in the Army must change our culture, reach out to IAF and augment our resources with the force multipliers of IAF. To their credit IAF has responded favourably every time their help has been sought. Simultaneously Indian Air Force also has to shun their attitude of we are here, if you want anything you come to me attitude. Look at the recent publications of US Air Force on Irregular Warfare and US Joint Publication on Close Air Support. Otherwise IAF would keep preparing for the conventional war but will be left out of battle in the present ongoing sub conventional warfare which the nation is fighting everyday as part of the Long War.

Sensors and Weapon Related Technology

Sensors. There are various types of sensors available for conventional operations. Sensors like Unattended Ground Sensors(UGS), Battlefield Surveillance Radar(BFSR), Hand Held Thermal Imaging(HHTI) devices, LORROS, TI - OE and short and medium range surveillance devices should be deployed in grid concept to cover the important approaches of infiltration and crucial areas. Efficacy of the same by Border Security Force (BSF) in North East should be explored.

Technology should be developed to provide wide-area coverage for trace detection of explosive chemicals and for efficient monitoring of waste streams such as garbage and sewage. Given the widespread use of roadside IEDs, sensors are needed that can detect changes and disturbances in road and ground surfaces and ground penetration at standoff distances.

Passive Night Vision devices (PNVD). We should be flooded with PNVDs. We should be king of the night in CI Ops. All ambush parties, patrols, sentries must have adequate number of PNVDs so that complete spectrum is scanned and kept under observation. Terrorists should be scared to move at night because of our dominance at night with night vision devices.

Small Camouflaged Cameras, Listening Devices and Bugs. Commercial bugs are available off the shelf. Our specific requirements can always be met by civil industry. Necessary modifications, if required, can be carried out. If these devices are placed in key areas or suspected places and soldiers are kept available within reasonable distance arrival of suspected militants can be detected and then taken care of. Organisations like Confederation of Indian Industries(CII) can play a big role if Army decides to procure/custom make these devices.

Unmanned Ground Vehicles. Unmanned ground vehicles are not as advanced as UAVs, but they are starting to play a growing role as well. In Iraq and Afghanistan, the U.S. Army and Marine Corps have used robots with names like PackBot, Matilda, Andros and Swords to search tunnels, caves and buildings for enemy fighters and explosives. They move on treads

or wheels, climb over obstacles with the aid of flippers, mount stairs, peep through windows and peer into caves with cameras and infrared sensors, sniff for chemical agents and even operate a small ground-penetrating radar.

BPJ. The existing Bullet Proof Jackets (BPJ) are poor man's alternative. Surely our soldiers deserve better protection with lighter and breathable BPJs. Same is applicable with Bullet Proof Patkas (BPPs).

MPV. Existing Mine Protection Vehicles (MPVs) are too large and high. Lighter and more maneuverable vehicles can be procured.

Destruction of Targets

Weapon Profile. The weapon profile of Rashtra Rifles (RR) battalions suit the CI requirements. Is there a point in changing the weapon profile of infantry units engaged in CI Ops? When are we going to get rid of SMC and use more potent and effective Machine Pistols? More and better quality flamethrower should be available. Technology can be misleading. A weapon using Laser at night illuminates the firer and become easy target of insurgents. Sniper Rifles with much better Passive Night Vision Devices and longer range would be welcome.

Unconventional Means. Americans in OIF and Russian in Chechniya and Beslan have used gas effectively to flush out terrorists. As terrorists would not have gas masks, gases like CS could be used. To flush out holed up terrorists in a mosque tear gas shells borrowed from local civil police was successfully used in J and K.

When a cache of arms and ammunition are recovered, we may not try to capture or destroy them. Use some spray on the ammunition (which are available and being used by US Army) so that the insurgent would not readily notice but would cause it to jam the weapons when they want to use it. Similarly we can use some bugging devices in the weapon cache and track the man with the weapon when he takes out the weapons. Idea is to catch the man behind the machine.

Own Measures

Signal Intelligence. Signal Intelligence units carry out interception of insurgent radio communications. However, with availability of cell phone and satellite phones insurgent groups have shifted/would be shifting to these means of communication. Insurgent groups in North East close to Bangladesh border even use Bangladesh cell phones. Same is applicable in J&K where terrorist orgs are using own as well as Pak cell phone communications.

The present ground realities have been succinctly put forward by Deputy Inspector General (Ops) of CRPF NC Nathanewal in Srinagar on 29 November 2007, in his presentation on "New Formats of Militancy and Violence in Valley". He said," They have online terror training

through which they try to motivate more and more youth. Besides they use e mails, SMS and mobiles for information and operation purposes. Earlier we could intercept emails through servers, but now they are operating through a single mail address at two different places. They pass the password in a code message and use the same account which makes it difficult to intercept."

Government of India is alive to the security issues. Since service providers of Blue Tooth technology do not come under the home ministry security scanner there is a proposal recently of not allowing these service providers to operate in India.

Insurgent groups all realize that the most secure technology for command and control is not technology at all. The insurgents, all with access to phones and radios, concluded that the safest form of communication was personal contact. A courier cannot be intercepted by the most sophisticated signal intelligence (SIGINT) means, a secret meeting cannot be monitored and a whisper in the ear of a comrade cannot be deciphered by the most sophisticated code breaking program.

Money Laundering. No insurgency or proxy war can sustain itself without money supply from outside. Terrorist groups will continue to adapt the way they raise and move funds as they deem necessary to evade governmental scrutiny. Government must closely monitor evolving trends in terrorist financing and develop effective strategies to respond quickly. Combating terrorist financing must also remain an important component of every government's counterterrorism strategy. However, the situation is complicated as money laundering is not illegal in most nations and transactional data are not required to "follow the money." That means anonymous transfers of money are both possible and likely. Authorities have to look to find the sources of terrorism financing in donors, nongovernmental organizations and criminal enterprises who all fund terrorist causes. In today's world of plastic money and hawala transactions inflow of money can be tracked provided inter ministerial cooperation between Finance, Defence and Home Ministries are in synch with requirement and technical expertise is put into place. The feeling in the CI battlefield is that sufficient efforts are not forthcoming in this very important aspect.

Data Mining. Due to grater transparency in the working of the Government, mushrooming of online journals and newspapers and TV channels, availability of the print media, specialised journals and research products of Think Tanks on the Internet make available huge volume of useful data to the terrorists. As we are trying to use Open Source Intelligence (OSI) the terrorists are also doing the same. To counter this internal information should be carefully monitored. What is available in the open media including internet must be carefully chosen. The kind of data, which the terrorists can now get with the help of the Internet search engines, is as follows:-

- Details regarding sensitive infrastructure such as the location etc of sensitive Government offices, banks and other financial institutions, stock exchanges, power stations, nuclear establishments, airports, railway stations, traffic choke-points etc

- Reports of parliamentary proceedings.
- Details of parliamentary and other enquiries into the functioning of intelligence and security agencies which often highlight their deficiencies.
- Case studies of important terrorist incidents giving details of how the terrorists operated.
- Case studies of the successes and failures of the counter-terrorism agencies.
- Testimonies given by intelligence and security managers before parliamentary hearings.
- Articles on arms, ammunition, different kinds of explosives, weapons of mass destruction material etc
- Articles on the counter-terrorism methods of the intelligence and security agencies.
- Articles on the threat and vulnerability perception of the security agencies etc.

IED. Remote Controlled Improvised Explosive Devices (IED) are causing the greatest concern all over the world for armed forces fighting insurgency. All terrorist organisations have been increasingly using IEDs. The methods for detection and neutralisation used by the counter-terrorism agencies have not been able to keep pace with the rapid changes in the modus operandi used by the terrorists. We must make use of the latest technology available in the world markets as well as indigenous resources to tackle the menace effectively. Surprisingly insurgents in North East do not use remote control. They prefer use of wire or some pressure/pull device to detonate. No electronic means can counter this type of IED and countering them becomes that much more difficult.

Information Warfare

Technology plays a very important part in information warfare activity in CI Ops. Electronic Warfare, Computer Network Operations, Psychological Warfare, Deception Operations , Perception Management, Intruder Operations et al are heavily dependent on technology.

Information is a tool, but the user needs to know how to wield it. Unfortunately, terrorists in Iraq, Afghanistan, Pakistan and elsewhere seem to make better use of the information available to them in support of their strategies than do forces countering them, despite the latter's more advanced information systems. With easy access to public information infrastructure-especially cellular networks and the Internet—they can operate in distributed but connected cells, reduce their vulnerability, increase their lethality, communicate with the contested population, learn from global insurgency experience and exploit media coverage, all the while hiding their tracks in the Internet. Against such networked and IT savvy adversaries, information power has to be more important than firepower.

Cautionary Thoughts.

The Limits of Technological Supremacy. The changes in military power wrought by the information revolution are in their early stages and they still have serious limitations. Even the

best surveillance systems can be stymied by simple countermeasures like camouflage, smoke, and decoys, by bad weather or by terrain like the deep sea, mountains or jungles. Sensors have limited ability to penetrate solid objects, so that they cannot tell what is happening in underground bunkers. Urban areas present a particularly difficult challenge: There are far more things to track (individuals) and far more obstructions (buildings, vehicles, trees, signs) than at sea or in the sky. Figuring out whether a person is a civilian or an insurgent is a lot harder than figuring out whether an unidentified aircraft is a civilian airliner or an enemy fighter. It is harder still to figure out how many enemy soldiers will resist or what stratagems they will employ. No machine has yet been invented that can penetrate human thought processes. Even with the best equipment in the world, U.S. forces frequently have been surprised by their adversaries. U.S. soldiers have been ambushed by insurgents who managed to elude their sensor networks through such simple expedients as communicating via messengers, not cell phones.

We should never forget that technology cannot be a panacea for fighting CI Ops. When fighting uphill in the mud or snow at night or in an ambush or storming a built up area it will always be the man behind the machine and not the speed of the processor which will be the battle winning factor. It is easy to use computers to help "warriors of the map", like staff officers at division HQs (maps, orders, tables). Once computerized, info can be easily transmitted to others. It is much more difficult to help warriors in contact. Their eyes and hands are busy and not with their computers. They talk a different language, not the language of the map but the language of contact. With GPS Locator and rangefinder/compass it is easy to feed location of point/enemy looked at. But what about the identification and description of the point looked at? This information would rarely be fed by regular infantrymen. It is likely to be fed only by specialists. When radios were heavy and bulky commanders were given a radio operator, now should we give him a C2-man? Multiple sightings of the same enemy (made by different people or at different times) would be the order of the day. Friendly troops may be sighted as enemy. Out-of-date display information will be misleading. Situational Awareness may be at "macro", not "micro" level. Some of the issues which merit attention are as under :-

- Hand held computers (PDAs) are likely to be in pockets during the fire fight. Leaders will devote more attention to his display only when he would anyhow stop, observe, think.
- Can't watch display and terrain at the same time with the Helmet-mounted displays.
- Watching information versus feeding information.
- Though it is easy to feed self-location automatically using GPS what about the accuracy when under a roof? GPS can be manipulated also.

Cultural Change. Utilisation of technologies is a command function. Nobody will ever deny the soldier their courage under fire and the skills to engage the insurgents. But we must

provide them with the technological wherewithal to carry out their tasks better. Technology is becoming cheaper, easier to use and fantastic facilities are on offer.

We are in the business of counterinsurgency for more than 50 years. We still do not have proper knowledge bank on CI Ops, there is no forum available where people can exchange their experience of this highly challenging and dangerous operations. In US Army officers quickly realized the need of such a forum and created websites like companycommand .com or platoonleader.com in internet and these sites have become hugely popular. The website of companycommand .com is given at Appendix C. In 2006 Lebanon War Israeli Army had a system of delivering Lessons Learnt to their troops from ongoing battle almost on line about the tactics, techniques and procedures of Hizbollah fighters. Our men are street smart, intelligent, innovative with powerful observation capabilities. Every Paltan has their own battle drills and methods to operate in CI Ops. But how do our junior officers and men share the knowledge acquired over last 50 years of fighting CI Ops?

Headquarter Northern Command actively involved in CI/CT Ops has taken the lead in Knowledge Management. Through the Northern Command website in army intranet a knowledge bank has been created which can be accessed by all formation headquarters of Indian Army and a very large number of units. A blog site Share Your Experience has been created for people to share their experiences involved in active CI/CT Ops. Response remains poor, a lot remains to be done but at least a start has been made. This can only get better.

Conclusion

In general counter insurgency planners have been successful when they were able to match or exceed the technological skills of the terrorist adversaries. We have to be ahead of insurgents on the issue, but it will require greater ingenuity and resourcefulness. Intelligence Database can be made available on Army Intranet and people wanting information should be able to “goggle” it. We can update the maps, which have historical data with superimposition of real time data and imagery and census information so that we can get activity patterns. Indian software skills are acknowledged world over. Technology is here. We have to make this technology work for our CI Ops. Obstacles are difficult to remove. The huge bureaucracy both within and outside Army, organisations like Controller of Defence Accounts(CDA) and Integrated Financial Advisers, eagerness of DRDO to raise hands for developing everything on earth and then failing to meet the dateline et al are difficult to surmount. Procurement under Army Commanders Special Financial Power (ACSFP) is so cumbersome that one feels that the procurement be done by normal conventional process under the aegis of MGO Branch. Hundreds of crores of rupees are required to be spent under a total ad hoc arrangement. While concerned Ministry of Defence officials may gloat over the stringent procedures given in Defence Procurement Manual (DPM) 2006 soldiers on ground who urgently require night vision devices, hand held UAVs, BPJs, helmets etc cannot be provided the same due to these bureaucratic procedures. Though terrorist related violence in 2007 has been the lowest since 1990 in our efforts to minimize collateral damage ratio of own troops to terrorists consults has shown an upward trend. We should never forget that the CI Ops is being fought in unit level 24x7, 365 days a year without any respite. Security forces are buying

casualties some of them are avoidable if we provide our troops the wherewithal. We must ensure every conceivable technical support for them. It is our job to overcome these hurdles. Troops engaged in CI Ops deserve nothing less than this. In army's higher hierarchy every one has tremendous experience in CI Ops. It goes beyond any logic when we are spending $ 2.7 billion for aircraft carrier Admiral Groshokov for Indian Navy, similar amount for Procurement of modern aircrafts for an eventual war in future but cannot give our troops, fighting the Long and deadly war everyday, the basic minimum requirement of say Night vision devices at a miniscule fraction cost of say Admiral Groshokov. Otherwise, forgetting out OODA looping (Observe, Orient, Decide, Act- Boyd's decision making cycle) insurgents, we will remain bogged down in procurement loop.

However we are not the only ones facing this dilemma. USA whose defence expenditure is almost equal to the rest of the world also has the same problem. Gen. James Conway, USMC, on 17 May, 2007 stated," We know that MRAPs save lives…So with that knowledge, how do you not see it as a moral imperative to get as many [of] those vehicles to theater as rapidly as you can?...I just see it's absolutely critically important to us to push this vehicle as hard as we can so that we save lives, in the process perhaps convince the American people that we can get after this casualty thing in a real fashion and maybe buy more time on the part of our countrymen to get this thing settled."

But in the final analysis, having the best technology is not enough to defeat the most committed terrorists armed with the deadliest weapons. Some of the most expensive weapons systems being purchased by the United States and its allies are irrelevant to fighting and winning the war against terrorism. To deal with the essential paradox of the information age—that the march of advanced technology may decrease our security in some areas while increasing it in others—we need not just better machines but also the right organizations, training, and leadership to take advantage of them.

Appendix A

Analysis of Insurgent Group

Some of the Factors for Consideration / Questions may be:-

- What is group's topology?Ethno-Nationalist?Nationalism separatist? Religious extremist? Jihadi?Extremist communists?
- What is the group ideological narrative /manifesto?
- What are the group strategic goals? Political? Religious? Societal?
- What goals has the group emphasized?
- What are the root causes and core motivation of group militancy? What are the specific grievances of the group?
- How sweeping are the goals? In the group pursuing revolutionary change a pursuit of specific goals.
- What is the structure of the group – cellular, hierarchical, home grown and networked? Is it a combination of these?
- What is the nature of leadership – Charismatic, committee leadership, quasi-military hierarchy and leaders movement?
- How much control does the leadership exercise over group operation, planning and strategies?
- Is the group operationally entrepreneurial and adaptive or does it act only when ordered by leadership?
- How cohesive is the group? Are there dissenting members and potential for splinter groups?
- How committed, subservient and professional are the members vis-à-vis leadership orders?
- How unique cultural factors, norms and behaviours significantly affected internal behaviour?

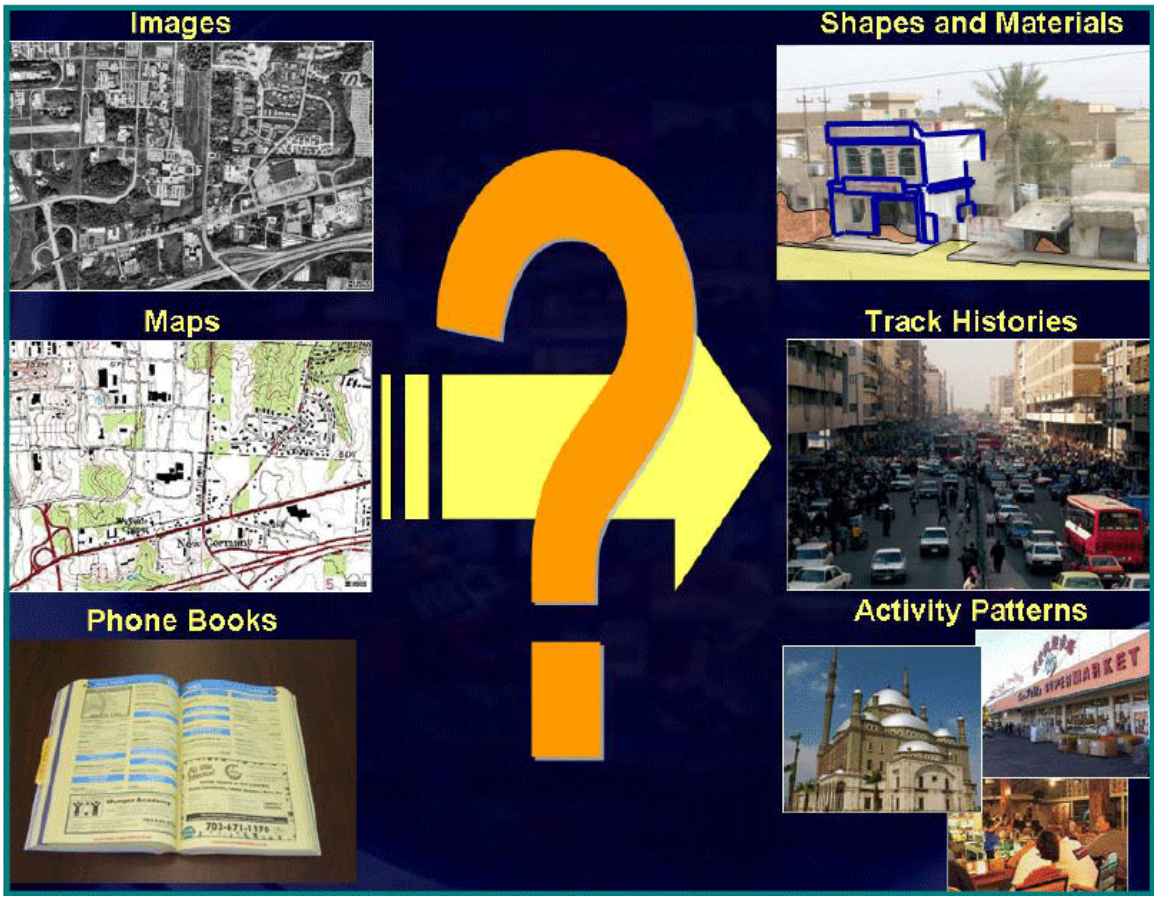
- What are the group's operational capabilities in term of :-

    - Number of figures and support operatives.
    - Militant training and expertise.
    - Weapons caches.
    - External or societal support.

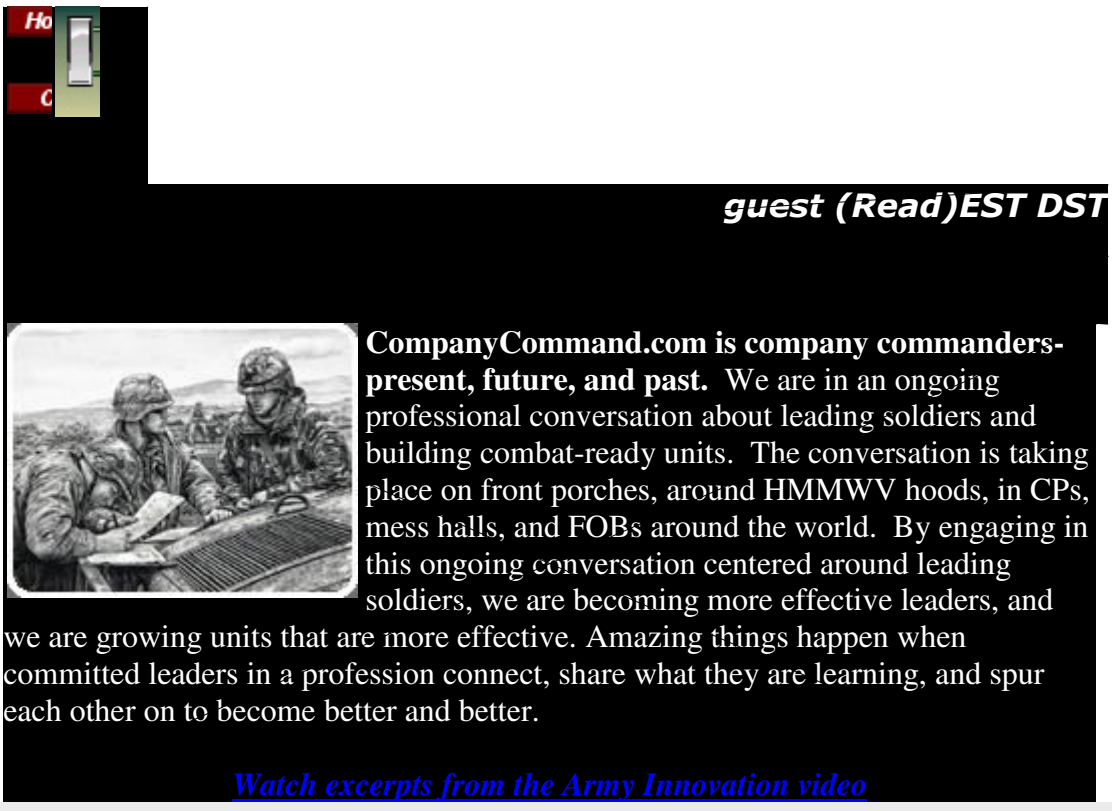
- What levels of operational sophistication and complexity have the attack demonstrated?
- Have any group operational failed? If so, how and why?

Appendix B

Map with 3D Model



Appendix C


guest (Read)EST DST
CompanyCommand.com is company commanders-present, future, and past. We are in an ongoing professional conversation about leading soldiers and building combat-ready units. The conversation is taking place on front porches, around HMMWV hoods, in CPs, mess halls, and FOBs around the world. By engaging in this ongoing conversation centered around leading soldiers, we are becoming more effective leaders, and we are growing units that are more effective. Amazing things happen when committed leaders in a profession connect, share what they are learning, and spur each other on to become better and better.
Watch excerpts from the Army Innovation video
LOGIN
CompanyCommand is a professional forum for U.S. Army Company-Level Commanders. You must be a logged-in member to participate. Membership is manually approved and is available only to Company-Level Commanders as well as currently commissioned officers who are either preparing for command or who have commanded in the past

Username

Password

Remember my login

LOGIN

Request Account

Login Problems?!?

and desire to contribute to current company commanders.

CompanyCommand Members: Login and connect with your comrades

END NOTES

1. B. Raman, From Internet to Islamnet: Net-centric Counter-Terrorism, Paper presented at a conference jointly organized by the State Islamic University (UIN) of Jakarta and the Institute for Defence Analyses (IDA) of Washington DC at Bali, Indonesia, from October 19 to 21, 2005,available at web site of Observer Research Foundation http://www.observerindia.com

2. K.P.S. Gill, Technology, Terror & A Thoughtless State, available at www.satp.org

3. David C. Gompert and John Gordon IV, War by Other Means, Published 2008 by the RAND Corporation, 1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138, available at http://www.rand.org.

4. Kanchan Lakshman, Jammu and Kashmir Respite from Proxy War, Faultlines : Writings on Conflict and Resolution, available at www.satp.org

5. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, http://www.nap.edu/catalog/10415.html

6. Dr Robert Tenny, ISR in Urban Environment, available at www. darpa.mil/ixo.

7. Inputs from our foremost counter insurgency and counter terrorism expert Lt Gen J R Mukherjee, PVSM, AVSM, VSM (Retd) is gratefully acknowledged.