Informationising of the Indian Army:
Need for Internal Reform

PC Katoch

Informationising

The term informationising draws global attention not because the Chinese coined it but because of the institutionalised accelerated pace at which the People's Liberation Army (PLA) is getting informationised as part of the revolution in military affairs (RMA). The Pakistan Army is following suit with focussed investments in relevant sectors, aided amongst other factors by the US [courtesy the global war on terror (GWOT)] and China. Significantly, the planned reorganisation of the Pakistan Army's GHQ (General Headquarters) envisages merger of the Communications Branch into the Information Systems Branch. In contrast, the Indian Army (IA) has yet to fully accept the essential requirement of viewing information from the strategic viewpoint and recognise it as a mission critical resource. In its concerted efforts to modernise, the IA must align with this truth and stop treating information as just another resource. Unless this vital step is taken, shedding the baggage of legacy thinking, ushering required critical advantage in information warfare would not be possible. With existing mindsets, even the goal of achieving net-centric warfare (NCW) capabilities faces constant slippages, negating capacity building. There is an urgent need for internal reform for which some hard decisions are required.

What constitutes informationising in an army? Essentially, it is the confluence of the Operational Information System (OIS), Management Information System

Lieutenant General **P C Katoch** (Retd) is former Director General, Information Systems, Army HQ.

(MIS), Geographical Information System (GIS), their integration with systems like the Electronic Warfare System (EWS) and Electronic Intelligence (ELINT), Logistics Management System (LMS), information assurance, including cyber security, automation and digitisation, e-war gaming and simulation, e-learning, e-procurement, on-line audit and the like, all with matching communications that enable real-time / near real-time exchange of information, including during fast paced operations.

In its concerted efforts to modernise, the IA must align with this truth and stop treating information as just another resource.

In the context of the IA, at the heart of informationising lies the Tactical Command, Control, Communications and Information (Tac C3I) System. Within the Tac C3I, the sub-systems of Command Information Decision Support System (CIDSS), Battlefield Support System (BSS), Artillery Command Control and Communications System (CCCS), Air Defence Control and Reporting System (ADC&RS) and Battlefield Management System (BMS) are all bound by the CIDSS as the backbone, also configured to integrate systems like the EWS and ELINT. Sub-systems of Tac C3I are in varied stages of implementation; from already fielded to request for proposal (RFP) for Phase 1 yet to be issued. Above the CIDSS (top end being the Corps HQ) is the Army Strategic Operational Information Dissemination System (ASTROIDS). MIS too are in various stages of development. Communications planned for exchange of information are the Tactical Communications System (TCS) and the Defence Communications Network (DCN), other than the Army Intranet on which applications like the Army Wide Area Network (AWAN) function. The TCS is also to integrate the mobile phone network of the army. War-gaming, simulation and information assurance are at very nascent stages. E-learning has hit a roadblock with the Army Intranet still not made secure albeit AWAN messages are being sent on it without a security solution being in place. On-line audit has been fully introduced in the Indian Air Force (IAF) but the IA is not yet game for it, citing security concerns.

Implementation of Tac C3I has been facing excruciating delays with stiff resistance from certain quarters; not recognising mission criticality of information and more for fear of loss of individual turf and dilution of the comfort zone. Though the Directorate General of Information Systems (DGIS) is charged with facilitating transformation of the IA into a dynamic network-centric force, achieving information superiority through effective management of information technology, it cannot do this in the requisite time without cooperation within the Integrated HQ (IHQ) of the Ministry of Defence (MoD) (Army). Presently, DGIS suffers from lack of breathing space and hierarchical intransigence to this state of affairs, adversely impacting informationising of the IA.

GIS and Military Survey

In an international seminar during 2009, a participating DIG BSF (director general border security, force) demonstrated a GIS that had been introduced in the BSF. He stated that this happened after the BSF acquired it from the Military Survey. It is a shame that GIS is still to be fielded by the IA. A GIS policy and Tri-Service Common Symbology was issued by the IA only in 2009, though the Military Survey was under Military Operations till 2005. This was after some 18 months of a comprehensive study that included Engineers and sister Services. Yet, Engineers tried to block its issue even at the last moment, fearing loss of turf. It is for the same reason that the draft RFP for an Enterprise GIS (approved in principle for fielding up to corps level) has been circulating within IHQ of the MoD (Army) for the past 11 months, with little accountability by those stonewalling it. Post fielding of the Enterprise GIS, the next phase is to take it down to the tactical battle area (TBA) followed by the establishment of a spatial data infrastructure (SDI).

The Military Survey came under DGIS in 2005 on the express directions of the Raksha Mantri for valid reasons of ensuring synergy of GIS with OIS and MIS. The Mapping Policy of India clearly states that the Survey of India (SoI) is responsible for the issue of all maps within the Indian borders, including Defence Series Maps (DSMs) but provision of maps by SoI and their updating is years behind schedule, quoting lack of manpower with SoI and delayed book debit payments by the government. This, despite a sub-unit of the Military Survey at Agra with dedicated IAF reconnaissance aircraft (they do not fly within 10 km of the border) undertaking SoI tasks and SoI making no payments to the MoD in return. Instead of ensuring that SoI delivers on their mandate, the Military Survey has been involved in the production of the DSM series maps (the task of the SoI) and physical survey for collection of attribute data, albeit conveniently ignoring insurgency areas. The undue emphasis on a physical survey needs to be viewed in the context of satellite imagery and modern technology, plus the fact that no physical survey is possible for trans-border maps where the actual battles will be fought. Computer-based digital techniques of handling geo-spatial terrain information and GIS as an efficient

Computer-based digital techniques of handling geo-spatial terrain information and GIS as an efficient decision support tool can well handle modern warfare efficiently.

decision support tool can well handle modern warfare efficiently. Technology provides new methods for preparing digital terrain data for both digital and paper maps.

The Military Survey follows an old system of 'reverse deputation' with the SoI. This was perhaps relevant in the initial stages when expertise in survey was limited. It needs to be replaced by a simple 'deputation' of 3-5 years, especially considering that this reverse deputation has hardly been practised in the last 25 years. The Military Survey on an average has been holding only 15-20 survey trained officers (these too mostly trained by the IA, not SoI) against an authorised strength of 103 survey trained officers over the last 25 years. Engineers hardly send officers on survey courses due shortages and such training is organised 'after' the officer joins the Military Survey. In the bargain, large numbers of Engineer officers in the SoI are in cushy jobs, and have attained major general rank – far more than they could hoped for within the IA. During 2009, when the turnover issue was raised by the DGIS, the SoI offered major general rank officers from the SoI to replace colonel level officers in the Military Survey. Incidentally, officials of the Ministry of Science & Technology privately admit that the SoI is one of the worst managed organisations.

The merger of Survey Sections at Corps HQ level with Indian Institutes of Technology (IITs) for creating GIS sub-units was approved through an army study in 2009. Engineers are loath to implement it, fearing loss of turf, and, feeling the heat under DGIS, want to move out the Military Survey; an issue that comes up time and again (including when the vice chief was from Engineers) especially when changes occur in hierarchy. How this can be justified to the Raksha Mantri is difficult to comprehend. The Engineer-in-Chief's Branch has no expertise in survey training. For such reason, no training instructions to the Military Survey had been issued for 10 years until this was pointed out in 2009. The Engineers also want to move DIGIT (Digital Survey Unit) under the Military Survey to Secunderabad, citing that DIGIT can interact with the engineering colleges. Such a move would be foolish. There are enough engineering colleges in Delhi. Besides, DIGIT must function in its present location under ADG Military Survey. The Key Location Plan (KLP) can easily come in vertically in the present location, accommodating the total requirements.

Contending Programmes

BMS vs F-INSAS The Battlefield Management System (BMS) and Future Infantry Soldier as a System (F-INSAS) programmes are under concurrent development, BMS under DGIS and F-INSAS under the infantry. BMS was conceived at battalion/regiment level pan army (including for the infantry) and comprises communication, non-communication hardware and software. The system will be further integrated with the Tac C3I through the CIDSS. Quite logically, Phase 3 of F-INSAS (computer sub-system, radio sub-system, software and software integration) should be part of BMS. However, the infantry has been given the go-ahead. A separate project of software and communication integration by the infantry will be retrograde, delay overall net-centricity pan army, incur additional avoidable costs and defeat the very purpose of creating DGIS, considerable work in the fields of applications having already been done by the latter in addition to completing Phase 1of CIDSS and BSS (Battlefield Surveillance System). Squabbling on delimitation between the BMS and F-INSAS cost a delay to Phase 1 of BMS by more than 12 months (an inexcusable folly, surprisingly supported by Military Operations). The Signals (whose role is to provide communications to Battalion HQ and above) supported the infantry, sensing they would get a role for provisioning communication equipment for F-INSAS. If infantry is to incorporate situational awareness and GIS, then it amounts to 'reinventing the wheel' and yet another project to integrate the F-INSAS with BMS with additional expenditure and time. Logic demands that for Phase 3 of F-INSAS, Project Management Organisation (PMO) F-INSAS should be placed under DGIS as part of BMS. The latter is also developing BMS for mechanised infantry, including in the dismounted role.

ASTROIDS and CIDSS vs AWAN After 13 years of ASTROIDS Phase 1 lying in a state of disuse, Military Operations transferred the project to DGIS for rejuvenation and initiation of the next phase. Yet, when the project was initiated, one of the road blocks being put was that with AWAN available, ASTROIDS were not required – showing a complete lack of understanding of technologies and applications involved! Similarly, CIDSS Phase II was stonewalled for eight months since Military Operations wanted the topology to be changed at the last minute at the behest of Signals. That would have delayed the project by a few years. Signals also feared competition with AWAN notwithstanding that AWAN enables only messaging albeit later versions of AWAN are to have voice and video facility too. In Military Operations, cases of information systems are largely dealt with by Signals officers headed by the ADG Information Warfare (IW) who too is a Signals officer. This bias needs to be corrected by having an all arms ADG IS (Information Systems) in Military Operations. This needs to be viewed as an essential enabler for accelerating informationising. Presently, even the implications of a Decision Support System (DSS) are ambiguous to many senior officers.

Cyber Security and Information Assurance In most armies of the world, information assurance (including cyber security) is handled by information systems. Signals quote that the Signal officer-in-chief was nominated chief security officer in 2004. The fact is that DGIS came into being only in December 2004. This anomaly needs to be rectified. Relating the existing capabilities of the Army Cyber Security Establishment (ACSE) to the information assurance control objectives clearly shows that only issues relating to personnel management and vulnerability management are being addressed and that too in a limited form. Other information assurance objectives of configuration management, secure software development management and verification management are practically not being addressed in any substantial measure. ACSE in its present form and alignment has a predominant "security of infrastructure" bias rather than the required bias towards "information assurance." The IA should take serious note of this. The capability to meet all information assurance objectives continues to remain fragmented because of our inability to centralise control over information assurance assets and the requisite collaboration between various stakeholders such as vendors/agencies undertaking development of information systems, project/programme management offices involved in deployment of information systems and users exploiting these information systems.

The IA needs to take concerted and early steps to address this gap in capability for meeting all information assurance objectives. An overall enterprise level Information Security and Assurance Strategy must be defined quickly. Based on this strategy, an enterprise level Information Security and Assurance Programme (ISAP) should be undertaken. It is vitally important to agglomerate existing organisations like the ACSE and other envisaged assets to create an Army Information Assurance Agency (AIAA) under the aegis of the DGIS to implement the ISAP. Unofficially, officers of ACSE opine that ACSE should have been part of DGIS. The IA simply has to be ruthless in following such an approach, disregarding protests of loss of turf by others. If we hesitate in taking such a step, the pace of modernisation can hardly be accelerated in the realm of information warfare. Further, stunted growth will imply inadequate cyber security and cyber warfare capabilities, severely restricting our combat potential. It would be prudent to make the DGIS a principal staff officer (PSO), bringing him directly under the vice chief. This would also help integrate systems like EWS and ELINT controlled by Military Operations and Military Intelligence respectively. In cyber security training, we should graduate from existing elementary to cyber security war-games where networks need to be kept operational under battle conditions while hackers try to infiltrate with methods that are likely to be used by our adversaries, including measures like flooding servers to block them, planting of viruses, etc. It goes without saying that information dominance must be an essential element of our war doctrine. We must be able to protect own information systems, attack / influence the information systems of adversaries and leverage own strengths to gain decisive advantage in a battlespace where national security is threatened.

The ACSE should expand to take on the role of Army Information Assurance Agency (AIAA). To ensure an organisation-wide ISAP, the AIAA must have necessary enablers to provide core competencies for gestating and sustaining the ISAP with sub-components of the Information Assurance Planning and Execution Division (IAPED), ACSE, Army Information System Testing & Audit Establishment (AIST&AE) and Army Information System Awareness & Training Establishment (AISA&TE). Presently, numerous applications are coming up throughout the IA, some of them without adequate security solutions and without reference and clearance from ACSE. This would jeopardise security once total networking is achieved.

In cyber security training, we should graduate from existing elementary to cyber security war-games where networks need to be kept operational under battle conditions while hackers try to infiltrate with methods that are likely to be used by our adversaries.

Data Handling and Data Storage Even some Signals officers are surprised that data handling and storage is being handled by Signals instead of the DGIS, these issues being the domain of the latter. Data collated and "filtered" laterally and vertically from designated information centres in a HQ would require being available to others in real-time. Analysis and identification of how much data or information can or will flow up, down and laterally across the echelons of command and organisation of boundaries is essential. An associated issue requiring attention is the security classification of data, which differs from printed material and has yet to be defined. Absence of a clear policy has resulted in data centres mushrooming all over. The Computerised Inventory Control Project (CICP) under the DG Ordnance Services by itself is going in for a Rs 400 crore data centre. Key concerns of optimal utilisation of resources, application integration, security and scalability can be met by establishing a Centralised Data Centre at Delhi. A Disaster Recovery (DR) Module, also to serve as an Alternate Centralised Data Centre, would be required at another geographical location. Centralised Data Centres at Command HQ level would be needed. Data centres should be underground with nuclear, biological, chemical (NBC) protection in Faraday modules with electro-magnetic pulse (EMP) protection. The Army HQ Computer Centre (AHCC) converted to Army HQ Data Centre (AHDC) needs to be made all arms and placed under DGIS. Eventually, the CICP Data Centre under construction should be converted into the AHDC, integrating all requirements.

Communications

Army Intranet

The Army Intranet is still to be made secure. This needs to be done at the earliest. Fixing responsibility with Signals took three years. There should be no ambiguity that security of communications is the responsibility of DG Signals. Securing the Army Intranet would open the floodgates of e-learning, including part courses instruction and professional exams on line. The IA also needs to review its policy of not providing the Army Intranet to tri-Service training institutions like the Defence Services Staff College and College of Defence Management (where almost 90 percent staff and students are from the army) and disconnecting HQ Integrated Defence Staff (IDS).

TCS

TCS, approved by three successive Raksha Mantris has still to see the light of day. It needs to be accelerated. The void has affected test-beds for Tac C3I sub systems. Designating a corps as a test-bed has little meaning if adequate communications cannot be provided. To date, all test-beds have been truncated, the disadvantages being obvious.

Communication Support for Tac C3I Sub-Systems

Lack of synergy between Signals and IS delays projects as the former, relying on existing terrestrial communications and legacy radios, needs repeated convincing, with accredited loss of time. Repeated arguments delay initiation of projects. Signals initially were loath to accept software define radios (SDRs) albeit they were not to 'replace legacy radios in totality'; SDRs with dual wavelength are available and can also communicate with legacy radios. The main problem with Signals is that they look at the bandwidth requirements based on communications in truncated test-beds, whereas prudence demands that we cater for communications for fast paced manoeuvre battles. It is no secret that the IA woke up late to the need of a dedicated satellite. As the largest user of space, the IA should have taken the lead to project such a requirement. The study on bandwidth requirement for the IA has been completed only recently at the behest of DGIS.

Communication Data Network System (CDNS)

The CDNS, commanded by a director level officer, is under DG Signals on the plea that it was created out of manpower ex Signals. Its role includes: to assist Tac C3I components in selection of communications equipment, interact with TCS, advise the component system on the choice of access media for connectivity to CIDSS, work on standards and protocols, advise on network security, network and spectrum management plus facilitate single window interface of DG Signals with all Tac C3I components. Placement of CDNS within DGIS will actually ensure greater jointness and viewing information from the strategic viewpoint instead of a biased Signals view.

DCN

Project DCN is to go down to corps/equivalent levels of the three Services. While the IA is in-charge of the project, providing the strategic communication highway, little is happening on the Services handshake for exchange of information. Presently, the process of defining common standards and protocols for the Services is progressing at a snail's pace at HQ IDS. It would also be prudent to go in for underground DCN nodes instead of overground, as planned, since these will be lucrative targets in the event of war.

Manpower and PMOs

Failure to view information from the strategic view-point has led to 'post office temporary posting' in DGIS. The last three directors general (including the present one) have been in transit, two of them holding the appointment from 7 to 10 months. Deputy DG level officers heading PMOs are also being shifted out after a couple of months. Director level officers already approved for promotion get posted in, only to move out within months. All this adversely affects projects that have long gestation periods. Expansion of the Army Software Development Centre (ASDC), approved in principle years back, has not been implemented. This needs to be expedited. The ASDC should be converted to an Army Software Management Centre and made part of the Army Information System Testing & Audit Establishment (AIST&AE) under the AIAA, as proposed above. The IA needs to consider long and dedicated tenures at least in organisations like ASDC and ACSE, including short service women cadres doing their entire / bulk service in such appointments.

War-Gaming and Simulation

WARDEC located within DGIS Enclave is under ARTRAC, not even under DG Military Training. The systems and applications are vintage using limited maps depicting terrain on own side of the border. The War-Gaming Centre at Chandimandir has progressed little. War-gaming should be planned on Tac C3I systems with integrated GIS of trans-border terrain where operations are envisaged. This should be the forte of the DGMT / DGIS while WARDEC could modernise for training on counter-insurgency / counter-terrorism plus war-gaming in training institutions like the Army War College.

Technology Voids

Electro-magnetic pulse (EMP) attacks (nuclear and non-nuclear) at critical times are a reality. This is a serious challenge. With technological advances and globalisation trends, systems and applications will continue to have foreign content no matter how miniscule. Adversaries can embed vulnerabilities (Trapdoors, Trojans, etc) in both hardware and software. We need to build capability for checking / testing and safeguarding against these. The Centre for Artificial Intelligence and Robotics (CAIR) has to exponentially increase the capacity to develop new and varied algorithms in order to keep pace with rapid induction of Tac C3I and other systems. The Scientific Advisory Group (SAG) must find ways and means to accord SAG approvals in a telescoped time-frame compared to the months / years being taken presently, resulting in inordinate delays in test-beds. We also need to speedily advance our chip manufacturing capabilities, a sphere in which we are decades behind China and which has serious implications for network security.

Conclusion

The IA needs to urgently review how it wants to treat information. Prudence demands we adopt an approach to establish information superiority at the earliest and plan to maintain / improve upon this edge. In the present environment, this appears a distant dream. There is crying need to take an overall view and make it 'top-down' changes. This alone can usher the required information revolution replacing the existing evolutionary approach.