Cyber Awareness for the Indian Army

CLAWS RESEARCH TEAM

The Indian Army jawan of today has higher levels of education and situational awareness than the state existing even a decade earlier. The average soldier joins as a matriculate with most aspiring to and achieving higher levels of qualifications during their service. Due to mass penetration of mobile phones with affordable network plans and the increasing number of soldiers using the computer and the internet, the way we work and interact with each other is rapidly changing. In many ways, the soldier of today is comfortable with technology and uses it productively, be it for banking, shopping, traveling, surfing or gaining information on a host of issues as diverse as medical problems or entertainment options.

In most aspects the Army is far ahead of its civilian counterparts, as they have been extensively using Global Positioning System (GPS) for navigation, secure Army Wide Area Network (AWAN) by those authorised, making computer aided presentations, using excel work sheets, MS word based bi-lingual correspondence, faxing, scanning, copying, print functions, reception of pay by e-clearance via core banking and e-shopping via Canteen Stores Departments (CSD`s), etc. The soldier in his quest for knowledge enhancement is aided by the organisation through tie ups with reputed institutions like Indira Gandhi National Open University (IGNOU) project 'GYANDEEP', Army College of Engineering, Management institutes, Army Education Corps run Human Resource Development Centre (HRDC) and such like varied education platforms with host of centres around the country enabling quality education for the soldier and his wards. The modern day soldier and his wards are, by and large, increasingly interested in operating GSM/ CDMA/ Wi-Fi/ wire line (with 2G/3G) network enabling solutions on symbian/android etc platforms.

In the Army, therefore, e-awareness and rapid proliferation of equipment on a mega scale gives rise to the need to educate troops about safety and security measures to avoid breaches in security and e-scams. The soldier must be made aware of the e-laws, security mechanisms at national and organisational levels, and how to operate within this secure framework by adhering to key standard operating procedures. This could be done by basic training at unit level on current trends in computing, relevant aspects of internet and communication with special reference to security issues, types of media available, restrictions and advisories on hardware and software, usage trails, how to maintain accountability, cross-checking and verification methods and reporting procedures. Special e-cadre classes should be instituted and specific training programs incorporated as part of unit held cadres and promotion examinations. Those with talent could be earmarked for higher levels of training. This would add to the overall skill level of the Army. We could also consider E-AWWA for the families to enhance awareness levels in the environment. Here, the service officers' wives could play a pivotal role.

As there is a wide variety of hardware and software availability in the open market, it may be prudent to make the same available via DGS&D route or 'against firm demand' (AFD) sections via the Canteen Stores Department (CSD). This would ensure internal, off the shelf, availability of items in a systematic manner with quality control being ensured and security and affordability aspects looked after. It would also be easier to maintain purchase records, study purchase patterns and minimise instances of sub-standard, 'compromised' software being inadvertently procured. A policy formulation could be carried out by DGIS, QMG`s Branch, (with reps of CSD) and the Corps of Signals to set this procedure in place.

Basic guidelines on disposal/ destruction with requisite safeguards need to be disseminated to the soldier and his kith and kin so that maximum gain is achieved while re-cycling redundant hardware and software without compromising on organisation related and personal security. The discarded computers and cell phones/ related items rarely find themselves in the 'dustbin' but are likely to follow the scrap or 'resale-for-a-pittance' route.

Using correct updated knowledge, security awareness, secure economical procurement, correct maintenance, usage and subsequent disposal would go a long way in ensuring that our soldiers are adequately prepared to use hardware and software. In the current e-scenario, the soldier must be e-armed. Better by far to be e-shocked in e-peace than to be e-fried in e-hostility/war.