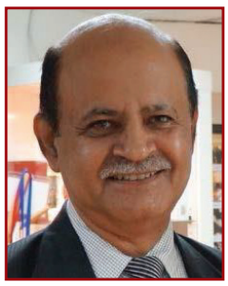
CENTRE FOR JOINT WARFARE STUDIES

SYNODOS PAPER | VOL - XIII NO-5 / APR 2019

# MAINSTREAMING CYBER ORG & TRAININGS FOR ARMY



**Lt Gen (Dr) SP Kochhar, AVSM**, SM, VSM (Retd) is a former Signal Officer in Chief, Indian Army. He is the CEO Telecom Sector Skill Council.**

## Cyber Defence-Organic

In each unit/fmn

- Basic training to all personnel
- Specialized Cyber Pl from unit upward
- Cyber staff wings at each HQ. They will coordinate and regulate cyber aspects.
- Cross movement/deputation to Cyber Offense teams based on aptitude and performance.

## Cyber Offense-Inorganic from existing resources

- Cyber wing at MO and IDS
- Cyber offense TFs-one each at Service HQ, Comd and Field Army

## 2 CENJOWS

- Cyber TA
- CERT

**Special Cyber Cadre- New raising under CT2**

- Uniformed
- Civil professionals
- Anonymous Cadre-Embodied portion of Cyber TA

**Trainings**

➢ **Pre-induction into Academies/ Training Centres**.

- GC's / Cadets - Level 4 of NSQF certification for IT literacy with basics of cyber.
- Recruits- Level 3 NSQF certification.

➢ **In Training Est**.

o A Cyber training wing catering to-

- Basic Cyber as relevant to the arm/service for all.
- Advanced capsule for recommended and selected trainees. Essential for induction into cyber Pl/ fmncyber branch, post DIPR based brain mapping test.
- Cater for up-skilling/ re-skilling going upto level 6 of NSQF level..

➢ **At Command Level**

o One Cyber range in the geography of each command to conduct NSQF level 7 and above courses under ARTRAC.

o Strong faculty presence, including international, to be ensured by guest faculty.

o Inductions into and out of the theatre to go through this facility.

o NSQF Level 7, 8 and 9 for selected candidates with minimum 3 years field experience.

- **Foreign language schools (to be manned by expatriates).**
  - To be set up as follows:
    - ✓ Train the Trainers- under ARTRAC
    - ✓ Train the Trainers- adjoint to the cyber ranges,
- **Special overt and covert cyber schools and ranges for cyber offense training.**
- **Set up and Funding**
  - Institutes adjunct to Training Est. to be set up in conjunction with MSDE and ESDM to train for pre-induction.
  - Basic NSQF Training to be financed by MoD.

## CONCEPT PAPER : HR & TRG

### Introduction

The needfor mainstreaming Cyber generally at National level and specifically at Military level requires to be clearly enunciated as this will dictate consequent HR policies and training. Cyber is going to become increasingly complex, withuniversal applicability across anything digital.

### Components of Cyber

Cyber may broadly be divided into the following aspects.

- **Defensive.**
  - This is for every individual, unit and fmn.It is more internalised and structured towards the entity being defended. It will include security of NWs, equipment, applicationsand data against external / internal threats, including threats from social media and cross platform communications.
  - There are advantages to tailor the organisation in an organic manner rather than another in-organic vertical. The reasoning for this is that since cyber is cross cutting across all domains, and yet is fundamentally enmeshed in each department's equipment, ethos and procedures / processes.Therefore, a standalone or deputation / tenure-based model will come to grief. Even though

the outcomes of cyber defence is the same for all, the pathways taken by different Services, and within the Services by each wing / arm/service will differ. The difference, therefore, will manifest itself repeatedly with each induction of networked device and process.

- Therefore, a dual tasked person who is constantly updated not only in the basic Arm / Service / Department he belongs to, but also on operationalising Cyber aspects as pertains to his stature, maybe a better asset than person from the same arm / service / department who is equally well trained in cyber aspects but sent on a tenure / deputation to a purely cyber dealing entity or Org. This is especially true for cyber defence and less for cyber offence.

- Taking the argument further, the career interest of this 'virtual' cadre will also be protected since they continue to work in their parent cadre albeit in cyber defence roles. Those who excel and have the aptitude can be transferred to the organisation tasked for cyber offence.

- Obviously, there will be a need to have dual reporting for this embedded cadre – one for their core arm/ service/ department and second for their cyber capabilities/ tasking. In this manner there will be no need to set up separate organizations at execution level and the requirement of additional manpower will be minimal. However, at the apex level i.e. MO/Dy Chief, a branch for Cyber Defence will need to be set up. This will entail having representatives of this cadre at each formation headquarters with a suitable rank. Cyber Defence should be inserted as a command function at each level of command to derive maximum benefit of this virtual cyber cadre within a cadre.

- It is suggested, that every unit maintains at least a section strength of such cyber qualified manpower. This will ensure career mobility as well as chain of command. Preferably every unit must have at least one such cyber trained officer. This slice of the cadre will have dual reporting- one through the traditional chain of command and second through the cyber chain of command, which will commence from the cyber officer to the cyber staff posted at each Headquarter reporting to the ADG level officer at MO and onto an additional Deputy Chief of IDS.

- **Offensive.**

This needs to be a centralised and specialised force, which needs to be coordinated at the national level and controlled at the highest level of the defence forces. The components for this tasking need to be vertical units / sub units. The recommended organisations are as given below

  - **Cyber Task Forces**. This would be a uniformed long deputation tenured Org scaled at the scale of one per field Army, Comd and Service HQ. This can report to the Dy Chief (Cyber) at IDS.The manpower will be drawn by selection from the Cyber Defence personnel discussed above to ensure technical competence in cyber aspects with contextualised application. Some of its taskings can be (not restricted to):

    - Intelligence Gathering.
    - Perception management and psy war.
    - Offensive cyber.

  - **Cyber TA (Hybrid Bridge)** In addition to the above, there will be a requirement of creating specialized unit where youngsters can be directly recruited based on their mental faculties, aptitude and geographical requirements. To bring them into the main stream and under the various defence acts, it is suggested that we create a cyber TA Bn. This unit can be an admix of personnel handling cyber in the military domain and in the civil domain. Hence, this will serve as a bridge between the two so that the National policies, knowledge and execution can be in concert with each other. This manpower can be of two types

    - **Core Group**. This should be composed of identifiable personnel drawn from Cyber Offense units and Cyber Defence Personnel.
    - **Embodied Group**. This component can be anonymous unidentifiable component of non-uniform wearing distributed youngsters mentioned above.

**Comd and Control Org.**

Cyber is another domain of warfare and we need to recognise it as such or give importance by creation of a separatewing / department at each HQ culminating in a Dy Chief at IDS.

## 6 CENJOWS

All personnel in this organisation need to be organic and not thrust as a tenure based individual. The tasking of this vertical would be akin to any line directorate.

There would also be a need to include a paragraph of cyber worthiness in the annual inspection report of the unit/ formation. Additionally, a specialized cell may be formed under the cyber vertical for carrying out discrete and random checks of cyber defence readiness of entities.

**Trg**

**IT Literacy**. For the organization to be cyber capable/ literate, it is necessary that the input to the cadre of all (Jawans and officers) should be pre-qualified in at least IT skills and if possible in soft-skills like communication skills. This can easily be accomplished by making the selected candidates undergo training and certification on these aspects in the time frame between selection and joining the Academy/ Training Centre respectively. The training will adhere to a Qualification Pack (QP) created for specific needs of the services. It is recommended that this QP is at level 3 or 4 of the National Skill Qualification Framework (NSQF). Suitable sandwich time frame can be given to a candidate to undergo this training prior to joining as a Cadet or Recruit. If suitably worked, these training can be imparted by institutes operated by ex-servicemen and funded by MSDE.

**Cyber Literacy and Competence at Induction.** On joining the training in Centres or Academies, every inductee will have to undergo a basic cyber foundation course tailored for that centre.This training is proposed to be embedded in every course of instruction across the board. Thereafter, each candidate will be subjected to a Psychometric test (to be developed by DIPR) to ascertain his suitability for cyber roles and associated aspects like confidentiality. Those who clear this test may undergo an additional cyber capsule of approximately three months duration and conforming to the next higher NSQF level, in addition to the common Cadet/ recruit training that is imparted traditionally. Thus, the pass outs who are cyber qualified may be given either a higher grade or additional increment to set them apart. However, they will be posted to organizations in a routine manner.

Thus, cyber training capability will have to be created at each training institution where both types of cyber training will happen with appropriate instructors.

**Building Cyber Competence by Apprenticeships / Upskilling / Reskilling**. We need to understand that a cyber specialist needs to have a flexible mind and a good insight

into the cyber/ software/ network aspects of relevant application and or equipment that is inducted into the cadre of which he is a part.

Therefore, there will be a requirement of getting experts as guest/adjunct faculty in our training facilities as also embed these personnel into the shop floors of the manufacturing industry providing the applications/ equipment and in foreign defence universities appropriately so that there is adequate knowledge of cyber vulnerabilities and opportunities of these entities. On return to the parent organization this knowledge will come in very handy.

While we have covered the entry level trainings and the specific industry training there will be a requirement of setting up skilling institutes, some of them anonymous, to re-skill and up-skill personnel so that they keep updated and there is adequate mobility vertically as well as horizontally. We recommend setting up one Cyber Range per Geography but under ARTRAC to conduct these theatres aligned specialised courses. These institutes should preferably be conforming to standards-based training which is based on NSQF levels which are approved by the cyber vertical of the service or at the national level by the cyber advisor. The functioning of these institutes should be entrusted to those personnel who are subjected to rigorous screening from the point of view of integrity, confidentiality and subject matter expertise.

**Language Trainings**. In addition to the above, there will be a requirement of setting up functional schools for training on relevant foreign languages by trustworthy expatriates of the relevant country.

**Structures Aiding Training**. There will be a need to create a Collaborative, Inclusive and Adaptive network of skill institutes which will range from common purpose to highly specialised (maybe covert) training centres imparting the above trainings. There may be a requirement of on boarding IB checks as well as accreditation by NBA equivalent confidential board. The funding of these trainings which will range from NSQF level 4 to NSQF level 9 may be explored from MSDE.

This network needs to be transformed into a digital technology enabled Hub and Spoke model of delivery of training based on Datawarehouse- Datamart structure overlaid with Rights and Privileges management by LDAP and OLAP. We need to build in trust and gradation using a private blockchain cloud. It maybe of benefit to create Fogs or Mini Clouds at each field Army / Service and seamlessly blend them into one enterprise cloud

using selected standards and protocols.

There will be a need to create a master pool of Master Instructors who will lead the trainings being delivered in the hub and spoke model using local vernacular speaking instructors at different places. This will bring in standardisation and normalisation using digital technology.

We will also need to create a digital content manufacturing facility to bring forth current and contextualised digital content flowing over the hub and spoke networks mentioned earlier. There will be a need to supplement this production wing with a subject matter pool and a research office.

It will pay dividends to consider introducing military Hackathons, competitions and awards to incentivise the seen face of the cyber work force both to attract fresh talent as well as to keep existing talent motivated. The Unseen face will also have to be equally incentivised by non-public disclosures.

## Conclusion

If the above outline is accepted, then there will be least amount of capital expenditure and cyber Defence capability will grow organically. Cyber offence and forensics will have to be in-organic. Maximum use of existing manpower, structures and processes has been factored in.

**Disclaimer**: Views expressed are of the author and do not necessarily reflect the views of CENJOWS



www.xtremeonline.in # 9811707220