STRATEGIC IMPERATIVES OF MILITARY NETWORKS: TOWARDS A CREDIBLE MILITARY CYBER POWER

M.K. SHARMA

INTRODUCTION

In the industrial age, post World War II, the indicators of the military might of any nation state have been robust military infrastructure, superior technology in platforms, weapon systems and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) backed by industrial vigour. Large scale infusion of the cyber element in military hardware has resulted in the development of relatively newer concepts such as Net-Centric Warfare (NCW). The Indian military forces aim to become NCW capable in the very near future with the Indian Air Force (IAF) leading the bandwagon. NCW enables application of C4ISR results in near real-time, thus, executing Effect-Based Operations (EBO) towards a decisive victory. The backbone to integrate all surface, air and space-based weapon platforms and sensors is the military network. One cannot imagine becoming NCW capable without ensuring a truly secure and robust network for integration of military assets. This is where the military networks come to centre-stage of cyber power building and enhancing the effectiveness of the armed forces.

Wing Commander **M.K. Sharma** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

The aim of this paper is to explore the strategic impact of military networks on military cyber power and how the Indian military Services should embrace military networks.

MILITARY CYBER POWER APPLICATION MATRIX

The conceptual framework to understand the impact of military cyber power on its concept of operations (con-ops) and actual mission accomplishments would be to see the military domain of cyber space as a sub-set of the global cyber space that enables the military. There are mainly two broad but blurring categories of networks with different attributes. The first category is of *open networks*, essentially driven by connectivity, whose measure of performance revolves around information sharing, collaboration and situational awareness. It permits a relatively higher latency in information transmission as compared to the almost real-time requirements in a sensor-to- shooter engagement. In other words, the importance of shared knowledge gain is more than the speed of operation.

The second and more important category is of *closed secure network*s where integrity of information, assured delivery and speed are most important tenets. The Integrated Air Command and Control System (IACCS)[11] and Voice Communication and Control System (VCCS) of the Air Force Net (AFNET) are examples of such secured close networks.

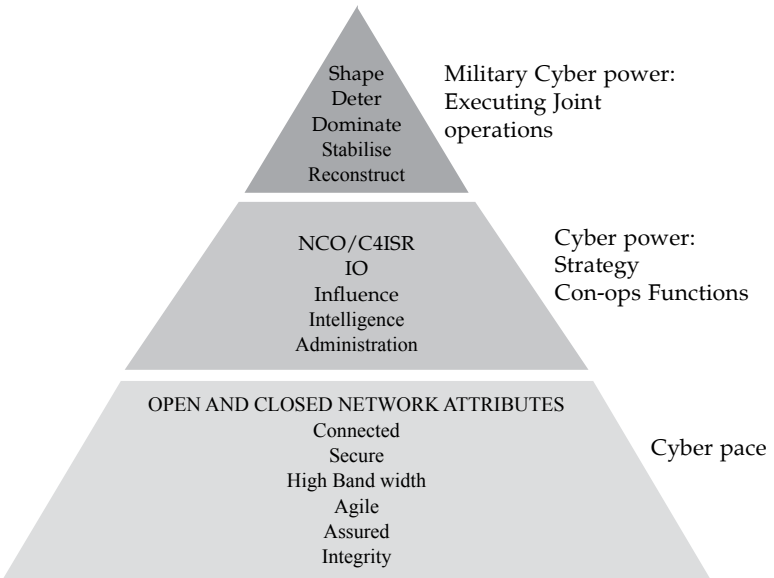
However, a closer look at the characteristics of the real world networks such as the Internet or any enterprise wide area network such as the AFNET, Army Wide Area Network (AWAN) or Navy Enterprise Wide Area Network (NEWN), would reveal that the open network and close network concepts do not apply directly, consistently and reliably. While the open network (i.e. Internet or a telecommunication network) is used to support some secure transmissions, a close network (e.g. AFNET) would

1. The Integrated Air Command and Control System (IACCS), an automated command and control system for Air Defence (AD) operations will ride the AFNET backbone, integrating all ground-based and airborne sensors, AD weapon systems and Command and Control (C2) nodes. Subsequent integration with other Service's networks and civil radars will provide an integrated air situation picture to operators to carry out the air defence role."IAF's AFNET NCW Backbone Goes Live Next Week" http://www.livefistdefence.com/2010/09/iafs-afnet-goes-live-next-week.html, accessed on February 3, 2014.

allow a lot of mundane, unclassified administrative communication.

The application of military cyber power could be either as a force multiplier in support of the kinetic war or purely against an enemy within cyber space itself. Military cyber power could be conceptualised as a pyramid whose base represents the domain of cyber space including the two types of networks with their attributes (Fig 1). It would depend upon the appropriate fashion in which these networks are employed for a specific military mission that would result in either a hard power or a soft power effect on the adversary. At the next level, resides the military cyber power that is enabled by the cyber space. This includes not only the strategy, con-ops, Net-Centric Operations (NCO) and Information Operations (IO) but also the combat support operations such as administration, logistics, training, personnel, planning, etc. All military missions prosecuted at various levels of preparedness (from pre-hostilities to the reconstruction stage) involving the use of cyber power are represented by the top portion of the pyramid.

Fig 1: Military Cyber Power in Support of Strategy, Con-ops and Functions



Adapted from: Elihu Zimet and Charles L.Barry "Military Service Overview," *Cyber Power and National Security*, ch. 12, pp. 290.

Information sharing enhances the quality of information and shared situational awareness that in effect enables collaboration and self-synchronisation, shortening the Observe, Orient, Decide Act (OODA) loop through increased speed of command, thus, dramatically improving mission effectiveness.

APPLICATION OF CYBER POWER IN JOINT MILITARY OPERATIONS

Planning and execution of joint operations is the key to success. This assumes more importance in the Low Intensity Conflict Operations (LICO) scenario where the armed forces may have to carry out punitive actions, peace-enforcement, peace-keeping operations and humanitarian assistance at the same time in different parts of the operation theatre. The role of cyber power to enable and synchronise hard power and soft power in support of such joint military operations include IO and NCO.

Information Operations

Electronic Warfare (EW), Psychological Operations (PSYOPS), military deception and Computer Network Operation (CNO) all reside under the wide umbrella of IO. CNO by itself consists of specific functions such as Computer Network Attack (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE). There are many associated functions that act as IO support operations, including physical security, physical attack, information assurance and counter-intelligence, etc. Also some soft military functions like public affairs, civil military operations or support of the military to public diplomacy are considered as related capabilities of a nation the for conduct of IO.

Net-Centric Operations

NCO is the enabling concept of military cyber power and the Indian military forces are poised to best utilise this growing facet of modern war-fighting by way of acquiring and developing systems to be more agile and adept. Information sharing enhances the quality of information and shared situational awareness that in effect enables collaboration and self -synchronisation, shortening the

Observe, Orient, Decide Act (OODA) loop through increased speed of command, thus, dramatically improving mission effectiveness. While both IO and NCO embrace the tenets of cyber power, their taxonomies are quite different. While IO is characterised by functionalities and operations, NCO is defined as capability, and is more concerned with enhanced speed of operations, shared decision-making, and mission effectiveness.

At the inter-Service level, the implementation of the backbone Information Technology (IT) infrastructure has not been done under a unified approach. The architecture of the enterprise wide area networks of the three Services has been developed in isolation.

The Challenges – Inter-Service

In execution of tri-Services joint operations, the application of cyber power raises some concerns on account of non -integrated technology platforms, stand-alone tailored view of NCW held by the air force, army and navy and variance in the Concept of Operations of the three Services. Let's take the technology non-integration issue. Broadly, non-integration exists at two levels: at the inter-Service level and intra-Service level. At the inter-Service level, the implementation of the backbone Information Technology (IT) infrastructure has not been done under a unified approach. The architecture of the enterprise wide area networks of the three Services has been developed in isolation, thus, may have variations in the Command and Control (C2) structure.

For instance, across the three Services the AFNET, NEWN and AWAN have been implemented as separate projects independent of each other. There have been a few Enterprise Resource Planning (ERP) implementations apart from messaging solutions within the Services with no common rules applicable across the Services. The navy was the first to implement a Commercially Off the Shelf (COTS) ERP for sailors and a home-grown ERP for General and Aviation Logistics. The air force has IMMOLS for logistics with no architectural similarity with the naval ERP on General and Aviation Logistics. The e-maintenance ERP for the air force is being implemented at a

cost of $55 million (approximately) and is aimed to connect critical aspects such as guided weapon systems, air defence radars, safety equipment, communication systems, armaments, mechanical transport of 170 bases, 550 units and 70,000 users to increase fleet availability to the optimum.[2] Absence of a unified approach while implementing such ERPs across the Services could prove to be the Achilles' heel as many common Air Defence (AD) radars, aircraft, missile systems, equipment and common spare parts are being used by the other Services whose availability, operational status, and logistics visibility would not be as transparent as desired for joint campaigns to take effect. Furthermore, the data format in which the required information is stored and transmitted may not be the same across the independent Intranets, making future "system-to-system talking" difficult. It demands more effort towards determining the technologies and procedures for common information sharing inter-Service.

The Challenges – Intra-Service

Intra-Service concerns of cyber power application are of security of the classified information critical to the mission's success. This takes prominence in spite of the fact that there is a centralised control of the access to information in respective solutions through administrator groups because presently, the numbers of such centralised applications are but a few. Practically, maximum amount of information is generated on work stations through a combination of office utilities like a word processor or a spread sheet.[3] While there are a few office packages on operating systems like Linux, the majority of the users use Microsoft Windows and MS office. In such a yet to mature Information and Communication Technology (ICT) environment, security of information raises some concerns as mentioned below.[4]

- Data created on a daily basis on each Personal Computer (PC) over a period of time builds up the information inventory with no automated

2. Sangeeta Saxena, "IAF Bases to Digitize Their Upkeep As Maintenance Command Turns 57", January 2011, http://www.indiastrategic.in/topstories853.htm
3. Commander Ashok Menon, "Electronic Document Handling in Armed Forces: Need for An Automated Approach", *USI Journal*, July- September 2012, pp. 432.
4. Ibid., p. 434.

mechanism to know the nature of content stored in that machine.

- Due to lack of any form of automation, there is a lack of visibility of document-inventory holding of the units/directorates/establishments. This implies that there is nil visibility on the amount of classified information held on each PC across the organisation – in absolute terms. Therefore, when an IT asset is lost, the organisation is at a loss to quantify how much/ how sensitive classified information might be in the hands of the enemy.
- While there are encryption tools on individual machines for the purpose of concealing classified information locally, there is no automated established mechanism to ensure mandatory use of such tools. The only method is the provision of physical check on each machine. This leaves room for the confidential/secret/top secret documents lying unencrypted on the workstations.
- There exists a lacuna that a lot of critical and confidential data condensed in the form of Excel files or an important justification in the form of a noting sheet/note of action/memo stored in MS word to support strategic/ tactical decision on deployment/acquisition of military equipment may be lying strewn on PCs across the organisation, in most cases unencrypted. The problem is further aggravated in the absence of an automated audit measurement tool to check the classified information held.
- With increased usage of Internet e-mail, it would not be wrong to assume that 'attachments' containing critical information are held in multiple work stations. This, apart from creating overheads in storage, more importantly, increases the risk of exposure due to leakage from multiple sources.[5]

PRAGMATIC UNDERSTANDING OF NET-CENTRIC WARFARE

While the positive correlation between the use of ICT and the effectiveness of the NCW concept is established empirically, many network architect experts are cautious of possible failure modes such as congestion collapse

5. "The Diverse and Exposing Digital Universe", IDC White Paper sponsored by EMC, March 2008.

or cascading failure. For instance, the US supported its 500,000 troops in Operation Desert Storm with 100 mbps bandwidth but in Operation Iraqi Freedom, the 350,000 war-fighters were supported by a huge 3,000 mbps satellite bandwidth. This provision of 30 times more bandwidth for a force 45 percent smaller, significantly improved the effectiveness of the platforms used. Essentially reiterating the primacy of good C4ISTAR (Command, Control, Communication, Computers, Intelligence, Surveillance, Target Acquisition and Reconnaissance) systems for the success of a joint military operation. On the other hand, since the NCW focusses so much on distributed information, the armed forces must be wary of the effects of the dissemination of false information entering the system, be it through enemy deception or simple error.[6] While the timely correct information could be a great force multiplier, the entry of incorrect/ misleading data into a system can jeopardise the expected mission outcome. This only gets aggravated by the non-linear pace of developments of artificial intelligence and other technologies.

While it is desirable to network every platform, system to the last soldier, as reflected in some Western literature, a country like India is not likely to afford such expenditure in the very near future. Then what should be the second best option towards becoming NCW capable? We should have a canopy of networks with a secure facility for storage of data and we should be able to securely and reliably deliver the required information to any person authorised to receive it at any place, at any time.[7]

CHALLENGES TO ASCENDANCY OF MILITARY CYBER POWER

Till the 1980s or so, the dependence of the Indian armed forces on civil infrastructure was restricted mainly to electrical power, railways and petroleum requirements. The requirement of weapons and communication systems would be met through the public sector. Other heavy military equipment like aircraft, tanks and ships was not embedded with intelligent systems though it was imported. Most of the military hardware comes with embedded electronic intelligence. Today, the Indian armed forces are sourcing a lot of their

6. Col R.K. Tyagi, *Understanding Cyber Warfare and its Implication for Indian Armed Forces* (New Delhi: Vij Books India, 2013), ch.11, p. 250.
7. Lt Gen Kochar, Chief (Sigs) at a seminar at USI on October 23, 2013.

requirements from private vendors, buying COTS equipment under various provisions of the Defence Procurement Procedure (DPP) 2013. For instance, under the 'Buy and Make (Indian)'[8] category of procurement, the private vendor in many cases may be just the front end of foreign manufacturers. The probability of embedding a malware by a foreign Original Equipment Manufacturer (OEM) at the behest of its government also becomes higher and easier as every weapon system or military equipment today has a 'cyber element' incorporated in it. This situation leaves India with the possibility of system disruption, and loss of command and control to exfiltration of sensitive classified information by other countries at the time of their choosing.

THREAT VECTORS IN MILITARY NETWORKS

While the drive towards digitisation, automation and interoperability is the name of the game in all the three Services, cyber security is not a mutually exclusive domain. The formula for risk assessment states: risk = threat x vulnerability x consequences. Therefore, to reduce risk, the effort would have to be on reducing any of the three variables in order to resolve the threat vectors. A deeper look into what is happening on the ground would take us to the 'real threat vectors'. Fred Schreier has identified four main threat vectors to military networks : supply chain and vendor access, remote access, proximity access and insider access.[9]

Supply Chain and Vendor Access

Supply chain and vendor operations are very difficult to monitor.[10] In a

8. Acquisitions covered under the 'Buy & Make (Indian)' decision would mean purchase from an Indian vendor (including an Indian company forming a joint venture/establishing production arrangement with the OEM), followed by licensed production/indigenous manufacture in the country. 'Buy & Make (Indian)' must have minimum 50 percent indigenous content on cost basis. This implies that indigenous content in the total of (i) Basic Cost of Equipment; (ii) Cost of Manufacturers' Recommended List of Spares; and (iii) Cost of Special Maintenance Tools and Special Test Equipment (reference parts 1(a), 1(c) and 1(d) of"Commercial Offer", Appendix G to Schedule I) must be at least 50 percent of the total contract value. In addition, such cases require minimum 30 percent indigenous Indian content in the first basic equipment made/assembled in India and in subsequent deliveries thereof, http://www.slideshare.net/agcool/dpp-2013 accessed on February 8, 2014.
9. Fred Schreier, on cyber Warfare, DACF Horizon 2015 Working Paper No. 7.
10. Tyagi, n. 6, p. 238.

global supply chain, it is very easy an adversary to manipulate the hardware and software by exploiting increased vulnerabilities. There exist many entry points vulnerable to injection of dormant capabilities starting at the factory floor itself in spite of availability of best quality practices. The next stages of manipulation arise at service delivery, wholesaler, the retailer, during installation and commissioning, during repair and even during downloading firmware update or patch. More importantly, these entry points are not restricted to the global supply chain only; they are equally applicable to the domestic logistic process, to a compromised soldier or to a Pakistani Intelligence Operative (PIO). The Services cannot afford but to innovate and invent new methods to address these vulnerabilities.

Remote Access

Ubiquitous application of Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) and firewalls to prevent network intrusion or hacking has put this remote access vulnerability as one of the top priorities of the system administrators and Network Operation Centres (NOCs). This heightened visibility can be attributed to the generation of overwhelmingly high quantity of warnings by the IDS/IPS and firewalls, coupled with the subsequent requirement of scanning through logs. However, hacking or remote access by a malicious attachment may or may not be the worst of the problems. This is where the Services have to strategise the response efforts so as not to exclude other equally insidious threat vectors that are not as visible to the administrator as hacking or network intrusion.

Proximity Access

This threat vector can be exemplified by 'interception of wireless signals' or programmes like Suter, developed by the Big Safari unit of the US Air Force that can monitor, jam and manipulate the data in any computer controlled network wirelessly. The suite can be carried on an airborne platform to get proximity to the victim network.[11] Basically, it is the adversary's ability to

11. http://www.defencenow.com/news/675/pan-india-optical-fibre-cable-network-for-defence-forces-at-an-additional-cost-of-$13-billion.html accessed on 23 Jan 14.

harm our cyber elements by being physically close to our systems without trespassing the defence premises. Though passive electronic communication monitoring, including phone tapping, is quite common, one of the most exploited liabilities in this regard is the wirelessly connected devices and access points. Terrorists use this vulnerability to their advantage very often. The advent of the Internet on mobiles with very low cyber security awareness is a boon to the terrorists /attackers. Even wireless key boards allow eavesdrops, broadcasting key strokes through the air, including, user id and passwords.

Though passive electronic communication monitoring, including phone tapping, is quite common, one of the most exploited liabilities in this regard is the wirelessly connected devices and access points. Terrorists use this vulnerability to their advantage very often.

Insider's Threat

Intrusion prevention devices and firewalls are like a hard outer shell that does not allow unauthorised visitors inside the network, but the employees, business partners and contractors have a unique advantage of operating from inside our physical and digital space without being challenged. If these insiders decide to attack, the consequences would be far-reaching as they know where are our mission critical jewels are kept, where the security gaps are, which security policies have not been implemented and when a key network security staff member would be away on leave, etc.

NETWORK FOR SPECTRUM (NFS): THE STRATEGIC IMPERATIVES OF IMPLEMENTATION

Military networks, unlike other commercial networks, assume strategic importance as they are tailored for a specific role to expedite decision -making with the highest security and reliability. Presently, the AFNET relies on the Bharat Sanchar Nigam Limited (BSNL) Optical Fibre Cables (OFC) network for transmission of information beyond the perimeters of the campus, thus,

The challenges peculiar to a military network are many, including delays in implementation, lack of architectural framework, security of military networks, high availability of networks, and mindset.

it is as vulnerable as the BSNL network. In order to reduce this dependence, the project 'Network For Spectrum' at the cost of INR 9,970 crore (US$ 2 billion approximately) has been launched to provide a dedicated and secure pan-India OFC network for the army, air force and navy. Incidentally, this would be the world's largest Closed User Group (CUG) network. The move has its background in vacation of 150 MHz of total 300 MHz of defence communication to the Department of Telecommunication (DOT) for use by commercial 3G networks. The proposed OFC network of over 60,000 km would provide connectivity to 129 army, 162 air force and 33 navy stations.[12]

While NFS would bolster the prerequisite of having an exclusive Intranet towards achieving end-to end cyber security, the enormousness of the network also throws up many challenges, technical and organisational, for the three Services to surmount. The armed forces, being the owner, provider and operator of the Intranet, have to secure the applications, data, systems and the network, unlike the commercial cyber security approach that is more inclined towards application-based cyber security. Furthermore, the challenges peculiar to a military network are many, including delays in implementation, lack of architectural framework, security of military networks, high availability of networks, and mindset.

Delayed Implementation

Moore's Law says that bandwidth requirement doubles every 18 months and the number of transistors that can be put on a chip doubles every two years. In such a scenario, unconscionable delays in implementation of ICT projects defeat the very purpose. The delay causes the old technology to get inducted in the Services at a higher cost and the maintenance of such

12. http://www.defencenow.com/news/675/pan-india-optical-fibre-cable-network-for-defence-forces-at-an-additional-cost-of-$13-billion.html accessed on January 23, 2014..

obsolete technology also gets limited support from the market in terms of non-availability of spares and expertise. There is a requirement of refining the procurement procedures, especially for ICT projects. Besides many other contributing factors, the delay is also caused on account of not setting up realistic Qualitative Requirements (QRs). The idealistic approach may not always be to our advantage. Specialisation is another factor that influences the project delivery time lines. Defence networking is a specialised task and must be handled by specialists from start to finish. The posting of tenure-based Human Resource (HR) management would cause more strategic harm besides visible delays.

Lack of Architectural Framework

The lack of a common architectural framework for all three defence Services will create incomprehensible complexities. Absence of the framework would make interoperability amongst the systems and platforms across the Services a difficult task. We need to have a common database definition, interface definition, standards' definition so as to create a universally compatible cohesive cyber eco-system. Wisdom lies in adopting the most widely used architectural framework called Department of Defence Architectural Framework (DoDAF) to suit our specific requirements. DoDAF Version 2.02 was released in August 2010 and is currently in use.[13] Many nations across the globe are using this open source architecture to their advantage.

Security of Military Networks

Military networks remain high value targets during both peace and war for obvious reasons. The air-gapped defence Intranets are not as secure as they were thought to be. The attack patterns are not limited to trojans/viruses/worms/logic bombs/phishing/spoofing/DDOS/PDOS, etc; the long-term organisational endeavours in the form of Advanced Persistent Threat (APT) could bring down almost any military network. For instance, the Stuxnet was used to infect computers known as the 'Industrial Control Systems' (ICS) used to programme and control the 'Programmable Logic Controller'

13. http://dodcio.defense.gov/dodaf20.aspx

(PLC) devices which, in turn, controlled the frequency converter drives that ran the centrifuges at Natanz, Iran, for enriching uranium.[14] The assigned target for Stuxnet was the Windows machine that was running the Step 7 software used to control PLCs manufactured by Siemens Corporation. To make it more precise, the PLCs needed to be a Siemens model 6ES7-315-2 controlling at least 33 frequency converter drives, manufactured by Fararo Paya in Tehran or by Vacon in Finland, running between 807 and 1,210 Hz.[15] This kind of lethality and precision was not seen in earlier versions of cyber weapons on the networks that are physically, electrically and electromagnetically isolated.

Also programmes like Suter[16], developed by the USAF unit 'Big Safari' can be put on an airborne platform and can penetrate a network wirelessly to not only monitor but also jam and manipulate the data. These pose another threat to securing military networks. Therefore, it is not enough to put Bulk Encryption Units (BEUs) and to 'air gap' the military networks to ensure security. Furthermore, the issues of security vs. convenience tradeoffs and standard vs. proprietary decisions would have to be weighed strategically. The approach to the security of a military network should be integrated and layered. The integration would have to be at least at two levels: the inter-Services network integration and the integration of tactical and strategic networks intra-Service. The security would have to be ensured not only at application level but at all the layers of the network, including physical, data link, transport and routing in order to provide sufficient defence in depth.

High Availability of Networks

The dependence of military operations demands a very high availability of the network. The concept of six 9s (i.e. 99.9999 percent availability of

14. "W32.Stuxnet Dossier", Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.
15. "W32.Stuxnet Dossier", Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>; and Dale G. Peterson, "Langner's Stuxnet Deep Dive S4 Video", Digital Bond, January 31, 2012, <www.digitalbond. com/2012/01/31/langners-stuxnet-deep-dive-s4-video/>.
16. http://www.airforce-technology.com/features/feature1625/feature1625-3.html

network) when translated on the ground means that a system should not be switched off for more than 30 minutes (including the off time for maintenance and breakdowns) during the whole year to achieve such a level of availability. Such requirements obviously place a high demand on resources like the standby power supplies, redundant systems and alternate buildings that is not feasible for every type of information that travels on the net. Therefore, the six 9s level of availability should be applied to all mission critical information systems and gradually the other mission non-critical information systems may be brought on board as the networks evolve and the economy of the country allows.[17]

There are two immediate and practical challenges to attaining six 9s availability: one is of the estimation tools and the other is of Service Level Agreements (SLAs) with third parties. The estimation of network availability requires specialised studies in risk mapping and system failure probability analysis that require software tools for automated monitoring of the networks over a period of time to ensure accuracy and reliability of the results. The SLAs require to factor-in the expected refusal of a civilian vendor to carry out repair/maintenance in the theatre of operations, therefore, development of in-house technical HR expertise to build self-reliance in terms of operating the network independently should take priority. Further, there are other challenges such as mobility, scalability, adaptability, etc that require inter-Service pragmatic understanding.

Mindset

While the technology pulls the organisation towards a flatter structure, the existing military set-up has always been hierarchical and would continue to be so. Therefore, the greater challenge for the leadership would be to maintain organisational hierarchy in a technically networked environment in order to get the best of both worlds. Furthermore, it is observed that automation tools are available to provide remote access, monitoring, authentication and paperless operations but we still find every PC having an operator sitting in front, physical teams visiting for IT audits and duplication through printing.

17. Lt Col Xavier, presentation at USI on October 23, 2013.

Ideally, we should have a proprietary network with our own standards and protocols for transmission of information but the question is whether that is a viable option?

The adage that technology provides a lean and mean force seems an elusive phenomenon. Till such time that mindsets change, the advantages that technology provides cannot be leveraged fully. As BH Liddell Hart puts it, "*The only thing harder than getting a new idea in the military mind is getting the old one out.*"

In order to embrace the current threat environment, the Indian armed forces would have to revamp their mindset that would drive HR policy, recruitment, training, postings, promotions and allocation of resources to achieve the attraction and retention of the best talent pool in the cyber domain. Without trained men/women behind the machine, the armed forces cannot exploit the capabilities of the network. Inclusion of cyber warfare in the curriculum of all training institutes including the *ab-initio* training schools of all air warriors/soldiers/sailors and the most elite warfare institutes of the Services is necessary for changing the existing mindset of considering a VOIP phone or computer as a communication tool, to a new mindset of regarding them as targets and weapons. Presently, all premier officers training institutes provide advanced training in domain specific forms of combat to a handful selected lot of officers.

Military leaders need to understand the uniqueness of end-to-end cyber security requirements of defence Intranets as against what the vendors propose according to their business convenience. The commercial communication has its evolution as 1G technology in the 1980s, 2G technology in the year 2000, and, presently, while India is taking advantage of 3G technology for spectral efficiency, the developed world is working on 4G LTE (fourth generation long-term evolution) and 4G LTE advanced to provide the customer with a more flexible environment. The militaries have also sojourned through their evolution from the concept of Revolution in Military Affairs (RMA) in the 1980s that aimed at digitising the battle space, to network enabled operations that relied on the availability of a common operating picture

in the form of information in the 1990s to battlefield command knowledge systems in the form of Net-Centric Warfare (NCW). The parallel drawn here is only analogous as militaries have moved through the concept of war-fighting based on the availability of data, information and knowledge unlike the specific 'generation of technology' in the case of commercial communication.

At the policy and strategy levels, the call on whether and how the cyber power could be employed would have to be taken by the Ministry of Defence (MoD). The time is propitious for the political leadership to debate on the issues of human rights, freedom of speech over national security interests against the background of growing cyber threats.

Strategic vs Tactical

The strategic networks would be more like the commercial networks in architecture with additional redundancies. However, the tactical networks are required for the conduct of actual operations and training exercises by seamlessly connecting the last weapon system/platform/soldier to the strategic network, the nodes of which are generally on peace-time static locations. Thus, the tactical networks demand different tenets, including mobility, portability, wireless connectivity, authenticity and reliability. How the last man/weapon system is able to trans-receive all the features like voice, messaging, intelligence or Global Information System (GIS) across the Services is the issue of technical interoperability that needs to be addressed. This is where a need is felt for a debate on whether to have a proprietary network or a standard network.

Standard vs Proprietary Network

Ideally, we should have a proprietary network with our own standards and protocols for transmission of information but the question is whether that is a viable option? Does India have the capability of doing so? The problem with this approach is at least three-fold: firstly, the cost involved in Research and Development (R&D) and implementation of such hardware and software would be prohibitive. Secondly, we will not be able to take

advantage of fast paced advancements in technology in the commercial world for spectral efficiency. And, finally, there would be continuous difficulty faced in maintaining, finding the manufacturer, and creation of updates for newfound vulnerabilities. On the other hand, the available standard network architectures do not have any of these demerits, including the cost factor. However, the security requirements of the tactical network demand a proprietary framework, therefore, the defence forces should adopt the standard framework and remain adept for specific requirements of defence by carrying out 'IT Asset Segregation'.

While the militaries, in their own way, are preparing for building India's cyber power by making robust their expanding network resources and employing other cyber defences for National Critical Infrastructure (NCI) protection, their contribution would only be seen at the operational and tactical levels. At the policy and strategy levels, the call on whether and how the cyber power could be employed would have to be taken by the Ministry of Defence (MoD). The time is propitious for the political leadership to debate on the issues of human rights, freedom of speech over national security interests against the background of growing cyber threats. As India moves forward to create its Cyber Command, the issues of the role and responsibility definitions of the different concerned departments e.g. the National Technical Research Organisation (NTRO) and the defence Services during both peace and war, are crucial to the success of future cyber operations. If the ultimate onus of waging kinetic war (when called upon to do so by the political leadership) and its outcome is on the defence Services, then it is only logical that they are provided the inputs through an institutionalised mechanism of information sharing rather than vice-versa. The MoD has to focus its attention on addressing these issues at the strategic level where capabilities can have the most profound effects.[18] There has been some serious effort in this direction, notably the release of three policy documents by the government: Crisis Management Plan for Countering

18. Somnath Mitra, 'Cyber Defence for Defence 2.0' Centre for Land Warfare Studies Article no. 2545, January 30, 2014. http://www.claws.in/Cyber-Defense-for-Defense-2.0-Somnath-Mitra.html

Cyber Attacks and Cyber Terrorism (March 2012), National Critical Information Infrastructure Protection NCIIPC (June 2013) and National Cyber Security Policy (July 2013). The military Services, on the other hand, are giving serious consideration to employment of offensive cyber power in support of their traditional operational and tactical roles. However, it is opined that the present policy, procedures and tools are not sufficiently robust to qualify for delegation of an outright offensive cyber authority beyond a very narrow scope.

National cyber power development is now a security imperative. There could be several approaches to legitimise, permit and authorise, the offensive use of cyber power against the targets deemed compliant with the Law of Armed Conflict. As a first step, the MoD, after defining the desired effects, could develop a plan for the defence forces to carry out cyber war experiments and exercises on a 'Cyber Weapons Testing Range' so developed, to explore the operational and tactical effectiveness of our cyber capabilities. This is not to suggest that the decision on offensive use of cyber power be made in haste, rather to get a realistic insight for both the policy-makers and defence forces in a 'top directed–bottom executed' approach to guide future employment of cyber tools. In a similar effort, for instance, the US has created Offensive Cyber Effects Operations (OCEO) and Defensive Cyber Effects Operations (DCEO) under the President's Policy Directive-20 that is set to authorise targets for cyber offensives, outside the geographic boundaries of the US.[19]

SOME RECOMMENDATIONS

The government's initiative for creating a tri-Services Cyber Command is a step in the right direction towards building defensive and offensive cyber warfare capabilities that could be employed at the operational and tactical levels. This is also in consonance with the recommendations of two independent study reports by the Institute for Defence Studies and Analyses

19. http://www.globalresearch.ca/obamas-cyberwarfare-first-strike-using-offensive-cyber-effects-operations-oceo-to-destabilize-countries/5338457 https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf

(IDSA)[20] and Data Security Council of India (DSCI).[21] The defence Services have to embrace ICT induced challenges by institutionally accommodating the growing training and educational needs specific to the cyber domain. Towards this, the steps would include induction of a dedicated cyber cadre at both Other Ranks (OR) and officer levels. Establishment of 'centres for cyber security' as a faculty at every training centre in all three Services that would impart essential *ab-initio* training on cyber security to all the recruits, would facilitate inclusion of cyber warfare awareness in military training. Also, establishment of a separate vertical as a School of Cyber Warfare Studies (SCWS) in the upcoming Indian National Defence University (INDU), with dedicated faculty at every institute [such as the National Defence College (NDC), College of Defence Management (CDM) and Defence Services Staff College (DSSC)] under it. This would go a long way in nurturing specialised cyber skills and developing a career path for such officers. SCWS at INDU would act as an incubator for embracing diverse thought processes and inter-Service cyber resource collaboration in military-like controlled and directed environments.

There is a justifiable case for raising exclusive cyber warfare units (as part of the Cyber Command) in various arms of the military Services. Such initiatives would require a more innovative talent management approach than the existing ones in order to attract the best talent and keep the HR environment apt for continued exploitation of their skills. Their terms of engagement, retention policies, expected work behaviour and incentives could be at variance with regulars. Specific areas that would be dealt with include encryption and cryptanalysis to build lawful interception capability, testing labs for accreditation of ICT products to mitigate risk arising from procurement of ICT products from foreign OEMs, cyber forensic and cyber crime investigation to build capacity of Law Enforcement Agencies (LEAs), Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), cyber surveillance and reconnaissance systems, cyber security research to cater for

20. http://www.idsa.in/system/files/book_indiacybersecurity.pdf
21. Comments on the 'Triad Of Policies To Drive A National Agenda For ICTE' http://www.dsci.in/sites/default/files/DSCI%20comments%20on%20TRIAD%20OF%20POLICIES%20TO%20DRIVE%20A%20NATIONAL%20AGENDA%20FOR%20ICTE%20v2.pdf

future NCI protection requirements and aspects of physical security of military networks.

CONCLUSION

Development of military cyber power is but an extension of the impact of cyber space on all elements of traditional national power. While cyber power has empowered militaries with NCW capability and precision weapons to a decisive advantage in the theatre of operations, the entities indulging in irregular warfare too have been empowered by the same cyber power. In fact, they have the potential of disrupting the NCI of any reasonably ICT dependent country like India. Cyber space is steadily becoming a pillar of our NCI. While the armed forces may own and command their tanks, missiles, ships, submarines and aircraft, they, nevertheless, have a limited share of ownership and command over Optical Fibre Cables (OFC), servers and satellites that run the information super highways.

As India prepares to protect its NCI, the government's cyber policy and cyber strategy initiatives in the last two years have been noteworthy, exhibiting national resolve to protect its NCI. The onus on the military Services to develop cyber power in its three dimensions—computer network defence, computer network attack and computer network exploitation —is but imperative. The military is also getting its much needed cyber resources in terms of a huge network infrastructure and other resources. Implementation of such a network demands strategic planning and due diligence in execution from the military leadership. Such efforts would have far-reaching consequences on the outcome at both operations and tactical levels in the future.

Despite the evidence of cyber weapons like the Stuxnet (or Duqu, Flame, Mediyes, etc) demonstrating the capability of entering the adversary's physical space and sort of legitimising the use of cyber weapons as a nation state activity, many still wish to relegate cyber warfare as just an irritant, on the pretext of its incapability of causing physical harm. Perhaps nothing could better describe such a mindset for dealing with the growing threat of cyber warfare than the old British Army adage "Proper Planning and Preparation Prevents Poor Piss Performance" (or the 7 Ps).