CMF IN CYBERSPACE DOMAIN

Air Marshall Daljit Singh, PVSM, AVSM, VM (Retd)*

Introduction

The world is witnessing disruptive technological developments especially in the fields of computer technology, communications, digitisation, and sensors, which have been well exploited by all. This new wave has generated a different operating space, known as 'Cyberspace'. Cyberspace is "*global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers*." [1]It is an open and complex environment which is easily accessible, and extensively employed in almost all domains by people, public and private organisations, governments as well as the armed forces.

In the public sector domain, energy, communications, railways, civil aviation, other transportation systems, banking, and financial institutes, are some of the major agencies employing cyberspace gainfully. All Private corporates dealing with Information Technology (IT), internet service, manufacturers and communication network providers are increasingly dependent on cyberspace domain for providing services.

The armed forces have embraced technological advances, suitably evolved operational concepts and acquired cyberspace based capabilities quite rapidly. They are well networked to exchange information, obtain real-time situational awareness, manage coordination, and take informed

decisions, which are conveyed at the speed of light. In fact, all other operational domains of land, sea, air, and space exceedingly depend on the cyberspace domain in all facets of operations.

Internet has been developed by design, to be open and easily accessible to the users, who could connect and share information through standard protocols. Internet security was neither considered seriously nor factored in establishing the connectivity norms. Today, cyberspace vulnerability is exploited copiously by rogue elements, state and non-state actors for ransom demands, cybercrime, cyber espionage, and cyberspace denial/ suppression of internet use. It is quite evident that more the dependence on cyberspace by any entity, more catastrophic would be the effect, if freedom of use of cyberspace is denied.

In recent armed conflicts worldwide, attacks in cyber domain are parallelly executed along with attacks in other domains, and their intensity would continue to increase as the dependence on cyberspace increases. The latest Ukraine-Russia conflict is the live example of this trend.

While India has software skilled force, cyber law enforcement agencies, emergency response and cyberspace monitoring agencies in place, they are all federated and work in their own verticals, resulting in sub-optimal countermeasures to the cyber threats, that threaten the national security. "*Defending against cyber-attacks demand cooperative approaches, collective efforts and pooling of resources, guided by policy guidelines*."[2] It is, therefore, important to examine the existing cyber environment, gaps and look at how India could ensure a robust, resilient, and superior offensive capability in cyberspace domain by exploiting civil-military fusion.

Present Civil Cyber Environment

As per Telecommunication Regulatory Authority of India (TRAI), there are 816.4 million broadband subscribers in India.[3]Due to digital transformation taking place, the internet penetration rate has reached 47 percent of the population. Information Technology (IT) is the growth engine of Indian economy and Indian enterprises have been providing IT services to other countries as India has large number of IT skilled,

motivated, and adaptive work force. Even sensitive organisations are connected to open internet domain, albeit in a restricted manner. Internet connectivity would continue to expand as the government is committed to expand the scope of Digital India, internet, and communications reaching the rural areas.

With exponential usage of cyberspace, there has been surge in cyber-attacks on governmental and other major private industries websites. The Indian Cyber Emergency Response Team (Cert In) detected and recorded 12.67 lakhs of cyber-attacks in the year 2022.[4] There are bound to be many more cyber-attacks going undetected and un-reported. The Government websites like DRDO, PMO and Department of Atomic Energy managed by National Informatics Centre (NIC), have been cyber attacked many times in the past, even though serious damage does not appear to have been done. The latest ransom attack on All India Institute of Medical Science (AIIMS) on 23 November 2022 had crippled the working of the Institute as medical records of four crore patients, including the medical records of the President, Prime Minister, other ministers, and top bureaucrats were lost and these records would be available for sale in dark web. Social media perception management is another area which has been copiously employed by people, terrorist organisations and other parties as an influence campaign. The Indian private and public agencies are gradually realising the urgent requirement to have more secure, robust, and resilient network with data retrieval backup.

Present Cyber Security Organisation and Legislation

India was one of the few countries to promulgate IT Act in the year 2000, duly amended in 2008 to deal with cyber threat. The National Cybersecurity Policy was published in 2013 (NCSP 13) mainly to bring out the government strategy to provide a "*secure and resilient cyberspace for citizens, businesses and Government*."[5]. The present cyber security organizations are established under diverse agencies of PMO, Meity, MHA and MoD. Under PMO, National Critical Information Infrastructure Protection Centre (NCIIP) has been formed to function under National Technical Research Organisation (NTRO). It facilitates protection of the Critical Information Infrastructure (CII), intelligence

collection, and extrapolating emerging and imminent threats in cyber space. The National Security Council Secretariat (NSCS) is entrusted with coordination of all cybersecurity issues, including cyber diplomacy. Under MeitY, Centre for Development of Applied Computing (CDAC), CERT In and National Informatics Centre (NIC) operate, to provide relevant developmental impetus and security response to a cyber-attack. MHA has a C&IS (Cyber & Information Security) Division. The primary role of National Intelligence Grid under MHA is to create a framework for data linking, data mining and analytics, issuing security guidelines for securing physical infrastructure and strengthening security measure. Under MoD, DRDO conducts research on technology-based software and hardware development for cyberspace applications. Reaction to the recent cyber-attack on AIIMS computer systems points to ambiguous and overlapping jurisdictions in protecting against, regulating, and investigating cyber-attacks. In this case, various agencies from MHA, CERT India, MietY, CBI, NIA, NTRO, DRDO, BEL and many other intelligence agencies came in to investigate the cyber-attack individually and investigating specific aspects[6]. There is a serious requirement for re-organisation of the cyber agencies to function under an umbrella organisation like Cyber Commission.

Indian Military Cyber Status

Cyberspace has matured into the fifth domain of war- fighting, which pervades other domains of land, sea air and space. Both state and non-state actors employ cyberspace as an asymmetric tool to conduct espionage, intelligence, and denial of service operations through cyberspace domain. Indian Armed Forces have been absorbing technological advances and they have moved ahead with netcentric operations, secure communications, and inducted smart sensor-fused and networked weapon systems. The Indian Air Force (IAF) was the first to operationalise Air Force Network (AFNET) in August 2010, which is the fiber optic network laid out throughout the country as the digital information grid under the 'Network for Spectrum' project. The IAF later operationlised Integrated Air Command and Control System (IACCS) which is an automated command and control (C2) system riding over the AFNET, in which, all IAF ground based, and airborne surveillance radars

are networked to provide composite air picture at all C2 nodes. With this networking, the IAF has achieved a high degree of netcentric operational capability. The IAF has been using software based Integrated Material Management Online System (IMMOLS) for long and has recently operationlised the automated electronic Maintenance Management System (eMMS). Indian Army has progressed in establishing strategic and tactical secure communication through Defence Communication Network (DCN), which will network all the elements from headquarters to field units through secure multi-spectral communications network. The Indian Navy has embraced netcentric operations by inducting Maritime Domain Awareness Software system and by integrating various sensors and C2 elements. All the services have employed data-linked and networked surveillance systems in various configurations. Cyberspace domain has been well employed by the armed forces while ensuring multiple layers of security.

To address cybersecurity issues, most of the software driven systems in the Armed Forces are isolated and 'air gapped' from open internet and all the three services have CERTs, monitoring data flow for intrusion at all the times. However, for updating the operating systems and other cyber hygiene measures, the systems would be net-connected in a sanitised environment. Exclusive optical fiber network provides some degree of intrusion protection to the networks. To ensure integrated approach to cyber security, the Government has approved establishment of Defence Cyber Agency (DCyA) to function under Chief of Defence Staff (CDS). The DCyA is tasked to handle cyber security threats for the armed forces and the manpower is pooled from all the three military services. This Establishment is the first step in consolidation cyber war capabilities and a lot more is required to follow.

Present Gaps in Military Cyber War Capabilities

- **Lack of Cyberwar Strategy**. Cyberwar involves actions to maintain freedom of action in cyberspace and deny the same to the adversary. These actions involve cyber surveillance of adversaries, ascertain their cyber vulnerabilities, shortlist potential targets (cyber intelligence), prepare cyber plans to degrade/disrupt hostile cyber

targets (offensive) and protect own cyberspace based assets against cyber-attacks (cyber defence). Hostile forces include states, non-state actors, terrorist organisations, independent or state sponsored cyber militia, against which the armed forces are required to protect their crucial war waging capabilities. Non attribution to the origin of attack and legislation gaps in defining the act of war, and ambiguity in the right to retaliate against such attacks, throw a lot of challenges to the armed forces in prosecuting offensive cyber operations.

- **India does not have clearly defined cyber war strategy**. NCSP-2013 has no mention of generation of national cyber power, and scope of cyber operations, especially offensive cyber operations, to be conducted against an adversary. Only cyber security has been the focus, leaving a wide gap in the national security strategy. Cyber deterrence is one of the effective strategies to dissuade and discourage other nations from cyber-attack. Deterrence by 'denial' to the adversary, by ensuring a robust and resilient cyber security is a prudent defensive strategy. However, offensive cyber capability is essential for effective deterrence and to cause prohibitive deterioration in cyber environment of the adversary. Today there are no defined cyber-attack 'triggers' which would authorise military action against the attacker. This a crucial gap in military cyber strategy.

- **Gap in Cyber War Organisation**. Defence Cyber Agency (DCyA) has been tasked with limited scope to ensure secure and resilient cyberspace for the armed forces, which is mainly defensive in nature and action. This scope and authority need to grow significantly with promulgation of Joint services Cyber Doctrine, strategy, equipping policies, training, recruiting cyber warriors, exercising and coordination with other civil agencies. At present, there appears to be ambiguity in organisational structure at headquarters, command and field levels, to the scope and authority for executing cyber war.

- **Gap in Skilled Manpower**. The armed Forces do not have the 'cyber specialist' cadre. The personnel employed in other jobs get trained to undertake cyber duties while manning CERT teams or undertaking other cyberspace management duties. The personnel, therefore, do

not achieve the required proficiency in cyberspace operations. There is a serious shortage of cyberspace trained manpower in the armed forces. The civil organisations have vast cache of trained personnel in many aspects of cyber security, software development, cyber audits, and cyber forensics. Many other countries employ trained civilians to conduct military cyber operations. Training expertise and cyber development for military operations would require substantial fusion with civil agencies, universities, and academia.

- **Gap in Military Cyber Intelligence**. Many civil cyber organisations like NTRO, NCIIP and NATGRID are mandated to monitor cyberspace environment against cyber threats and protection of critical infrastructure, however, there is no focus on cyber vulnerabilities of adversary militaries, which could be effectively targeted during operations. It requires consistent and continuous monitoring of potential targets in cyberspace, as, unlike physical targets where physical infrastructure can be located and is visible, the cyberspace based targets are more elusive, dynamic and the vulnerabilities could be plugged anytime.

- **Cyber R&D**. India has vast number of universities and other academic institutions where research and developmental work on various facets of cyber-security and computer technology is undertaken. The armed forces lack such facilities. The civil expertise could be well employed to support cyber war operations.

- **Dependence on Foreign Manufacturers**. Indian armed forces have been quite dependent on Foreign Original Equipment Manufacturers (OEM). Most of the fighters, secure communication systems, EW systems operational today, have Integrated semiconductor chips and back end software from foreign companies and OEMs have Intellectual Property Rights (IPR). This makes the armed forces dependent on OEM to update/upgrade the software, for which, they are given access to the systems. This increases the chances of the 'outsiders' meddling with operating systems which could be detrimental to the armed forces, especially in a networked environment. While this issue will continue to persist with already acquired systems, this

vulnerability would addressed through Defence Acquisition Policy 2020 (DAP 2020) issued on 30 Sep 2020, in which, indigenous front-end software has been insisted on and mechanism to safeguard cyber security issues has been addressed.[7]

- **Lack of Exposure to International Military Cyber Exercises.** The Indian armed forces have been engaging other foreign armed forces in military exercises dealing with HADR, anti-terror and other operational aspects. However, there has been no cyber operations themed exercise conducted so far. The US military has recently announced sixteen nation multilateral exercise in Africa, during which, cyber was exercised to defend cyber infrastructure and to operate under cyber-attack conditions.[8] Israel regularly conducts such exercises with the US and other friendly forces. Indian military would gain a lot by exercising in this field.

Way Forward

- **Promulgation of Military Cyberspace Strategy**. A comprehensive Military cyberspace Strategy (MSS), which should clearly define the mandate, and strategic missions for the military force, should be promulgated at the earliest. The national policy to treat any attack on national cyber sovereignty, as an act of war, and authorise armed forces the freedom of action of the full spectrum of offensive weapons including offensive cyber power, should be clearly defined in the strategy. This would convey our resolve and deter others against cyber-attacks. The armed forces would continue to plan and conduct cyber operations even without promulgation of MSS. However, MSS would provide clear roadmap and guideline to establish effective cyber war capabilities.

- **Cyber Intelligence**. Intelligence on cyber infrastructure of the adversary military, its vulnerabilities, weak links and cyber resilience and cyber war capability is crucial for the armed forces to plan all aspects of cyber war, especially the offensive operations. Cyber intelligence would be analysed along with Signals Intelligence, IMINT and HUMINT to generate comprehensive ‘target folders’. This should be collated at HQ IDS (DIA). DCyA should be the nodal agency

to coordinate with NTRO, NCIIP and NATGRID and convey the military intelligence requirements. Consultation with civil intelligence agencies would result in rich and actionable intelligence.

- **Offensive Cyber Plans**. Offensive Cyber plans follow a cycle of analysing cyber intelligence to assess weak and vulnerable areas in adversary cyberspace, ascertaining effective offensive cyber tools to shortlist the best options, gaming the cyber weapon and keeping the target under surveillance, to ensure existence of the vulnerable gap in target. Typical cyber targets would be networked Air Defence Systems, Command and Control Centres, Communication nodes, surveillance centres, satellite communications, critical military information infrastructure, maintenance support, administrative and logistic network. Cyber offensive would be synchronised with other tools of offensive operations including Electronic Warfare (EW) attacks, and physical attacks of cyber infrastructure. The armed forces must involve other governmental specialist agencies to ensure that cyber actions do not lead to uncontrolled and unintentional consequences, causing collateral damage and even cyber fratricide, especially in critical infrastructures. Civil support would be required to mask the cyber-attack trail. Specialists from other civil agencies should be involved in developing the most effective attack option.

- **International Cooperation**. India has signed MoUs with many countries on cooperation in cybersecurity defence cooperation. Ministry of External Affairs (MEA) and MoD should consider expanding the scope of cooperation to conduct joint military exercises and training in digital and cyber domain, to learn the nuances of cyber operations. The US and Israeli military conduct such exercises, regularly with other friendly countries.

- **Human Resource Training and Retention**. The armed forces must be authorised to recruit personnel in the ‘cyber specialist’ cadre. The terms and condition of the service should be introduced to ensure continued employment in cyber domain. Special retention bonus may be considered to retain the trained specialists, as is done in many other countries. The recruits should be trained at dedicated

Cyber School for the armed forces. Some specialist training could be outsourced to select civil universities and military related cyber training should be imparted at the dedicated Defence Cyber School. Senior leaders should be indoctrinated thoroughly on cyber security at civil organisations and on cyber war operations at military school, at regular intervals to update them on ongoing developments. HQ IDS should consider employing civil specialists for conduct of cyber operations. However, implications of laws of Armed Conflict should be clearly understood by the stakeholders.

- **Interaction with Defence Industry.** With emphasis on 'Atmanirbharta' in defence production, future induction of weapons and systems is likely to be from Indian companies and with embedded Indian software. Availability of indigenous software would ensure better software hygiene management and software up-dation in a secure and reliable cyber environment. The armed forces must continuously interact with Indian defence industry to appraise them of the armed forces requirements of interoperable data links, operating systems and computer hardware and firmware. Standardised systems communication protocols would ensure better connectivity amongst the three services. The armed forces must task CDAC and DRDO for research in the latest computer technologies.

- **Legislation and Cyber Laws**. Cyber operations must have legislative backing and legitimacy in conformity with international norms. There must be provisions to act against cyber offenders for which cyber laws must be in place to deal with cyber operations under laws of Armed Conflict and International Humanitarian Laws. Specialised civil agencies should be involved in their correct interpretation and applicability.

Conclusion.

Disruptive development in digitisation, computer technology, communications and networking has ushered in a new domain of cyberspace, in which the entire world is networked, information gets shared and massive stored data is instantaneously accessed.

Cyberspace is a common domain used by people, public and private industries, governments, and military, without any boundaries. Internet design has far exceeded its design objective of interconnecting all participants, without any restrictions. However, internet security was not considered during inception and now this standard and open internet protocol has been exploited by rogue elements for espionage, denial of service, ransomware, and frauds. Internet service providers prioritise financial and commercial gains which leave open gaps in cyber systems to be exploited by agencies with evil intent. Critical infrastructure that significantly impacts daily life of people and functioning of finance and commercial entities and government departments are vulnerable to cyber attacks. The government has laid down some policies and regulations to make cyberspace environment robust and resilient for economic stability and national security. Cyber-attacks, however, continue unabated with lethality and complexity increasing every day.

The armed forces have imbibed the modern technology and netcentric operations are the standard norms of all the armed forces. Cyberspace is now a new battlefield for military and cyber war has been regularly and parallelly waged along with other domains. Military or intelligence agencies of more than thirty nations have acquired cyber offensive capabilities.

As ninety percent of cyberspace usage is in civil domain, good cyber security expertise and skilled workforce are available in civil domain. The armed forces have been originally organised and structured for kinetic warfare in land, sea air and space domains. They require more impetus in skilled workforce, training, and research in cyberspace. The military requires national cyber approved cyber war strategy to prepare for effective cyber war and safeguard cyber critical infrastructure, ensure cyber deterrence, and acquire credible cyber offensive capability as crucial instrument of war. Civil-military fusion is, therefore, essential for the nation to acquire winning cyber war strategy. Military Cyberspace Strategy must be promulgated which authorises the armed forces to employ offensive cyber weapons in retaliation to any cyber-attack on the national critical infrastructure, people or military assets. The armed forc-

es require cooperation from civil agencies in training, cyber intelligence and cyber legislation and offensive cyber tools.

*__Air Marshal Daljit Singh, PVSM, AVSM, VM (Retd)__, is a former AOC-in-C, South Western Air Command and Assistant Chief of Air Staff (Air Defence) and Director General (Air Operations).

Endnotes

1 Defense Primer: Cyberspace Operations issued by Congressional Research Service, updated on 09 December 2022. https://sgp.fas.org/crs/natsec/IF10537.pdf accessed on 10 Dec 2022

2 Gp Capt Ashish k Gupta, Cyber War: Conquest over Elusive Enemy, p 141, Published by KW Publishers Pvt Ltd

3 India largest connected nation with over 800M broadband users: Rajeev Chandrasekhar, https://yourstory.com/2022/12/more-than-800-million-broadband-users- Medianama, Ayeshwaria Lakshmi updated on 12 Dec 22.

4. 12.67 Lakh Cyber Attacks Reported In India By November 2022: IT Ministry In Parliament, https://www.medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/ by Villari Sanzgiri accessed on 23 Dec 22

5 National Cyber security Policy issued on 02 Jul 2013 by Ministry of Electronics and IT

6 Who should be accountable for AIIMS poor cyber security, Hindustan Times, https://www.digitalsecure.in/post/who-should-be-accountability-for-aiims-poor-cyber-security,accessed on 22 Dec 22.

7 Defence Acquisition Policy 2020, para 13 Chapter II, page 25, issued on 30 Sep 2020 by Government of India, Ministry of Defence.

8 Cyber to be featured for the first time in US military Exercise in Africa, Colin Demarest,\https://www.c4isrnet.com/cyber/2022/12/22/cyber-to-be-featured-for-first-time-at-us-military-exercise-in-africa/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-cyber. Accessed on 28 Dec 2022.