Atmanirbhar Bharat: Establishing Credible National Cyber Capability

Colonel Suraksh Vir[@]

Abstract

Cyberspace is a man-made construct, thus, imperfect, and hence vulnerable. Vulnerabilities enable nation-states to exploit cyberspace for further national aims. Exploitation exists due to Western dominance in cyberspace systems, technology, services and software. Atmanirbharta (Self-reliance) and a few optimisations in cyber defence, exploitation and offensive capabilities shall enable credible cyber deterrence for a nation.

Introduction

With the advancement of networks and digitisation 'Cyberspace' has harnessed an independent construct and a domain for itself. At present, there are 14.4 billion connected devices globally compared to the roughly 8.1 billion population of the world. According to Cisco's new Annual Internet Report Forecast[1], by 2024, there will be more than three times more networked devices on Earth than humans. The ubiquitous and inescapable requirement of networks has opened an extra dimension of warfare/vulnerability for nation-states.

Vulnerability is the driving force in the cyber domain. They arise due to the gap between theory, practice and capabilities. The growing reliability of nations on digital networks, globalisation and accessibility from outside, make these vulnerabilities exploitable. Cyber offensive requires the targets to be accessible

[@]**Colonel Suraksh Vir** was commissioned in the Indian Army in the Corps of Signals on 06 Dec 1997. He is an alumnus of Indian Military Academy Dehradun, Military College of Telecommunication Engineering Mhow and Indian Institute of Technology Kharagpur (IIT K). He did his MTech in 'Electronics and Electrical Communication from IIT K in 2010. The officer has tenanted important staff appointments as Joint Director, Network for Spectrum Cell, Deputy Chief Signal Officer, Headquarter 11 Corps and Colonel Signals (Project management), in a Corps. As Commanding Officer, he raised a Corps Operating Signal Regiment from 2013 to 2016 and also Commanded a strategic Intelligence Unit from 2018 to 2022 where he was awarded Vice Chief of Army Commendation Card in 2021. He is pursuing a Research Fellowship from United Service Institution of India on 'Enhancing Offensive Cyber Capability at National Level'.

Journal of the United Service Institution of India, Vol. CLIV, No. 636, April-June 2024.

and possess vulnerabilities at the required time of engagement. The major impact of a cyber offensive is to create temporary confusion and frustration among the enemy.

Tenets of Information and Cyber Operations

In the era of an always connected, unregulated web environment (the majority being deep and dark web), it is impossible to remain unaffected by perceptions created for furthering national and international aims by nation-states. The advancement of the internet and networks has given birth to the 5th dimension of warfare in terms of Information Operations (IO). Thus, every nation shall endeavour to enhance its capabilities to achieve information superiority as a whole, wherein, cyberspace forms an integral and potent role.

Overt IO are the ones, wherein, the initiator takes ownership of such operations and seeks a visible advantage e.g., government advertisements promoting its policies or operations against cybercriminals etc. Covert IO are those where in the nation-state sponsorship is denied once exposed. Due to the convenient anonymity offered by cyberspace, it presents itself as an ideal choice for conducting covert IO and creates a viable cyber operations capability for a state. Accordingly, the capability enhancement in cyberspace has to be worked out in synergy with other verticals of IO and aims to achieve desired information supremacy.

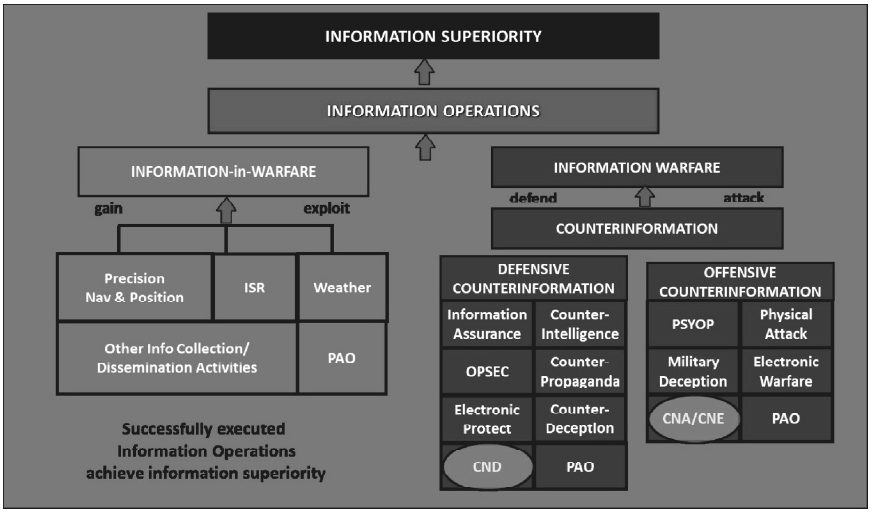

Figure: Tenets of Information Superiority [2]

Cyber deterrence refers to a nation's capability to dissuade potential adversaries from engaging in Cyber Network Exploitation (CNE) or Cyber Network Offensive (CNO) operations against its interests, while also enhancing its own Electronic Warfare (EW), kinetic, and satellite operations both strategically and tactically. It is achieved by presenting a credible demonstrated capability of severe counteraction and conveying to the adversary that the cost of all such actions shall outweigh its perceived gains. Cyber deterrence operations being a covert IO, come with a rider of appropriate countermeasures by adversaries, either physically or in the cyber domain. The ability of a nation to manoeuvre such IO and countermeasures to its advantage defines the cyber reliability and capability of the nation. Integrated cyber deterrence has emerged as an enabler in the overall deterrence capability of a nation.

The ability to create, identify and weaponise a particular vulnerability defines the cutting-edge potency of IO of the country. Thus, achieving self-reliance in the domain is a must for denying equal opportunity to adversaries and ensuring stable and robust cyber defence for one's own state.

Historical Perspective and Vulnerability Analysis: Western Dominance of Cyberspace

Due to the long occupation of India by the British and other European countries, as well as their global presence, the globe was left around to follow a Western legacy and align with Western systems and services. It was imperative and necessary at that point in time to follow suit due to inherent economic conditions and security issues. They left India with an education system which was primarily biased towards the West and the progress depended upon the utilisation of the systems and services offered accordingly.

The present-day internet comprises of networks and applications that are deployed and operated majorly by Western countries. Microsoft Windows, the world's most used Operating System (OS) with a global market fixed at approximately 65.0 per cent is based in Washington. Google, Gmail and Android have a maximum global presence with Headquarters (HQs) in California. Cisco Systems, Inc., and Juniper, the major world leaders in routers and networking, have HQs in San Jose and Sunnyvale,

respectively. Starlink, the pioneer in satellite-based Internet Service Provider is American. Though, these companies are private and commercial in nature, but their dependency at the time of conflict cannot be guaranteed due to political or nationalistic interests.

A recent example is the ongoing Russia-Ukraine conflict where Microsoft ensured a special release of Windows OS patches for Ukraine's Information and Communication Technology (ICT) systems. This was aimed at denying any advantage to Russian state hackers to unleash potent cyber-attacks. Another example is the free provision of Starlink-based internet to Ukraine.[3] The technology was instrumental in guiding Ukraine's drone strikes on Russian tanks and positions. Though later on the services were discontinued but such possibilities exist.

Maximum social media platforms with a global presence like WhatsApp, Facebook (Meta), X (Former Twitter) etc., are owned and located in the United States (US). It has to be granted to Western countries' vision in understanding and creating control on such platforms, even if it requires paying hefty prices. The purchase of Hotmail, the first web-based Email platform, co-developed by Mr Sabir Bhatia[4] (Indian) for USD 400.0 mn by Microsoft in 1997 and the recent takeover of Twitter by Elon Musk for USD 43.2 bn[5] in Oct 2022, etc., should not be viewed only as commercial ventures. The power of social media and email platforms in creating world perceptions and as a potent tool for hybrid/grey warfare and cyber exploitation is known to all.

However, now after 75 years of Independence and having established the foundation, as the 5th largest and evolving economy along with an inherent young, energetic demographic profile, Bharat is at the cusp of revolution in cyberspace. Bharat is an evolving nation with the second largest (800 million) digital population in the world. Bharat's tremendous success in the digital economy has been appreciated globally. It is with pride that CEOs of leading global Information Technology (IT) businesses (Microsoft, Google, Twitter till recently etc.,) are being headed and driven by Bharat nationals. Bharat's developer community is on an exponential rise, with the second largest developer community (13.2 million developers) presence on GitHub (a renowned online software developer platform)[6] and set to take over the US by 2027.

Developing nations, like Bharat, presently have to rely heavily on services, applications and systems offered by developed nations and, hence, the inherent vulnerability exists. In order to achieve true potential for creating a reliable cyber capability, it is imperative to have indigenous systems and software that can be fully relied upon and are free from any supply chain and propriety issues. It is an opportune time for Bharat to come forward and establish *Atmanirbharta* (Self-reliance) in software industry and systems in order to become a force to be reckoned with in the cyber domain and diplomacy, a vision it can easily achieve.

Need for *Atmanirbharta*

Viable and strong cyber capability stems from two inherent cyberspace components. First to have knowledge of the systems and services of adversaries with the capability to exploit their vulnerabilities at the time and effect of own choosing, and second, to have ownership and control of their own systems and services to be able to minimise damages in case of any offensive/counter-offensive by adversaries.

Except for China[7], (whose vision to stay untouched by Western influence and develop its own systems and services has paid rich dividends albeit at the cost of the privacy of its citizens), most of the Indian adversaries are on similar Western platforms and thus share similar vulnerabilities. Hence, it creates a level playing field for Bharat and a comprehensive and synergised approach to Cyber Network Defence (CND), CNE and CNO can achieve the required national cyber deterrence aims.

In order to achieve the same multiple measures need to be initiated by Bharat to optimise existing resources and expedite additional reforms. A case example is the development of Bharat's own GPS system, Navigation of Indian Constellation. The necessity arose due to the experience in the 1999 Kargil (Indo-Pak) conflict when US-based GPS data was denied to Bharat exposing the vulnerabilities of depending on foreign technologies and services. Accordingly, a few suggestions for achieving *Atmanirbharta* in cyberspace (CND, CNE and CNO) are as enumerated in the succeeding paragraphs.

Proposed *Atmanirbhar* Optimisations for Enhancing National Cyber Capability

Cyber Network Defence. A lot of improvement in CND has been achieved in the last five years with Bharat reaching among the top ten countries in the Cyber Security Index. However, with an exponential rise in technology and Artificial Intelligence (AI), a lot needs to be covered by the People, Process and Policy trident approach (especially with respect to awareness and education of people being the weakest link in the chain). The recent example being, the hacking of Microsoft Executive accounts by Russia, hacking of Las Vegas-based Caesars (a Casino giant) and Metro-Goldwyn-Mayer Resorts secure networks, made possible, due to simple social engineering exploits.

Own OS and Software. There is an urgent need to develop completely owned systems and services, especially for the Critical Information Infrastructure (CII) and defence services. In this regard, there is a pressing need to develop independent and hardened OS meeting the desired operational requirements. This shall avoid any dependence/ control by Western products through licensing issues or hidden bugs (which could be launched by the release of updates when required). The development of Bharat Operating System Solutions OS for e-procurement for defence is a beginner's step that requires further improvement and hardening to meet national aims. The in-house developed software and services shall also deny a level playing field to India's adversaries and further enhance the Cyber Security Index globally.

Addressing Supply Chain Issues. Bharat needs to develop indigenous capability for manufacturing its own hardware systems in order to avoid vulnerable supply chain issues. The gap in semiconductor and hardware manufacturing in the interim can be met by hiring such facilities in friendly developed countries by utilising positive diplomacy.[8] This requirement is immediate and urgent to deny a level playing field to any adversary and have a robust critical management plan. for example, the blacklisting of Huawei hardware by the US Government citing security concerns and its closeness to the Chinese government. In Aug 2023, US President Joe Biden passed an executive order that limits American investment in the Chinese semiconductor industry and AI companies to reduce its presence amidst the new anti-spying policy of China.

Enhanced Civil-Military Cooperation. Bharat's defence, technologists, business and corporates will have to collaborate, cooperate and create a comprehensive ecosystem for tackling technology-driven threats. These concerns were voiced in Singapore Cyber Week 2023, held in Oct 2023. There is a professional need for enhanced civil-military involvement as relying on half-baked in-house innovated software products is not only inefficient but also not in sync with the latest developments in the field. The task of experts and industry professional standards should be left to the same but with due diligence of requirements duly moderated by user department(s). The system integrators and manufacturers must be made equal partners through well-drawn contracts and legal frameworks and should be held accountable for the 'Availability' of systems. In this regard, the planning and establishment of the Centre for Cyber Operations and Security, a joint civil-military set-up, is a welcome step towards revolutionising the nation's approach towards addressing the emerging and exponentially increasing cyber threats.

Cyber Deception. Cyber Deception should be incorporated as part of active cyber defence. Presently, India's capability of cyber deception is in the initial stage, with negligible presence, thus, not much effective in support of credible cyber defence. There is a need to learn the craft and exploit it to the fullest in order to diffuse the attempts of adversaries before they even reach the CII.

Integrating AI in Cyber Defence. AI is emerging as a game changer in many fields and so are its advantages in cyberspace. The ability of AI to address things in real-time compared to human skill is a major advantage. The efficient AI probabilistic models and ability to compare the behaviour of the program contrary to its intended behaviour and creating depth in defence and controlling impact against an effective cyber breach shall act as revolutionary for all fields of cyberspace (CND, CNE and CNO).[9]

Old Inventory (Vintage Revival). A large IT inventory of the nation, especially defence services, is of old vintage with a lack of inventory management and rotation at formation levels. There is a serious need to review the active life of IT systems and their constant upgrades with the latest OS and other software to contain the breach and efficacy of information. Old vintage IT assets and

unsupported OS/software remain vulnerable to old and cheap exploits, which come in handy to any adversary in breaching the system at a low cost. Thus, moderation of the lifespan of IT assets shall dissuade adversaries from applying outdated low-cost exploits on Indian systems resulting in strong cyber defence.

Cyber Network Exploitation.

- The most useful and maximum utilised domain in cyberspace is CNE. It is predominantly passive in nature. The aim is to maintain a foothold in the compromised system and regularly gather intelligence or become a pivot for the furtherance of CNO/deterrence operations when desired. Due to the large data storage capacity of systems and mobiles, the compromise of these assets has assumed primary importance for carrying out any furtherance to Human Intelligence (HUMINT) operations in the overall canvas of espionage.

- Effective CNE capability keeps you abreast and competent to adversaries' vision/approach, thus, providing impetus to national and international diplomacy. The involvement of state and non-state actors (Civil Cyber Professionals [CCP]) in the field is no longer hidden. Having self-reliance in state-owned hardware, software and services minimises these risks. Though all nations follow sound practices, having a coordinated and synchronised effort acts as a force multiplier and minimises cyber fratricide along with the optimised cost to the state.

- Thus, there is an exigent need to identify the departments and agencies involved in similar tasks and efforts optimised by clubbing these agencies under a singular or a smaller number of disjointed efforts, meeting the aspiration of the nation at first and organisations at second. This shall also optimise the cost to the state and lead to the development/ procurement of better and more costly exploits and solutions leading to reduced cyber fratricide, improved utilisation of a limited talent pool, continuous cyber intelligence and better efficiency in line with national requirements.

Cyber Network Offensive/Deterrence.

- Cyber Offensive/Deterrence is the capability of a nation to execute a cyber-attack at its own will and time of engagement achieving the desired result with enough resilience to withhold or retaliate a counter-offensive by adversary, if any. Such actions are mostly covert in nature with non-repudiation, if exposed. The CNO is generally kept at a threshold in a manner so as not to escalate it to a level of physical retaliation by an adversary. CNO operations may also be incorporated and act as force multipliers along with EW and Kinetic operations during active war/counter-insurgency/counter-terrorism operations. A recent example being Israel, where it was put under a heavy cyber siege by Islamic hacktivist groups in the midst of Hamas rocket attacks.

- Such operations are largely preceded by CNE operations, thus the craft of successful CNE operations takes primary importance in the overall canvas of cyberspace. The primary targets of CNO are strategic in nature viz., industrial systems, large business centres, stock exchanges, power or nuclear grids, dams, hospitals, subways, banking systems, etc. Such attacks may lead to physical casualties also.

- Unlike CNE, in CNO operations the adversary gets first-hand information of such an attack and the vulnerability in the system is exposed. The adversary immediately reacts with precautionary and remedial measures in identifying and plugging of vulnerability. However, once identified, if feasible, the adversary may employ its own deterrence policy and launch a physical or cyber counterattack, if required. This also signifies the need for constant hopping and reconfiguration of IT assets employed for CNO.

Immediate Measures for Enhancing CNE/CNO Capability

Capacity and Policy Building.

- Develop standard operating procedures and escalation matrix for executing a cyber war.[10]

- Establish the required presence and resources in the deep and dark web and exploit the same for deception and intelligence.

- Establish a civil-military joint set-up by hiring appropriate and loyal non-state actors/CCPs to craft a transparent and equal playing dynamic cyber eco-system. Specialist CCP should be hired with assured career goals and remunerations to enhance the cutting edge in cyberspace. Few operations can also be outsourced selectively with due monitoring. Due checks and balances while integrating civilians should be given the highest priority in order to avoid the pilferage of critical and sensitive information by the likes of Edward Snowden and Yuri Bezmenov etc.

- Create and upskill indigenous capabilities in language, big data, analytics, AI, cryptology, network survivability and availability.

- Integrate CNE and CNO operations to address the challenge of limited availability of cyber-trained and capable personnel in defence, enhancing overall efficiency. The dispersion of cyber capabilities across various defence and civil agencies leads to competition for top talent among these organisations, causing friction and inefficiencies.

- Maintain readiness and dominance in an ever-changing information environment which will remain a major challenge. The integration across various elements is the key solution to achieve this aim. First and foremost there is a need to merge espionage and offensive disciplines across cyber, electronic and space warfare. The present arrangement ignores that these disciplines are heavily intertwined, utilise common resources, and shared reconnaissance and if left uncoordinated shall lead to serious cases of fratricides and conflicting objectives. Secondly, by integrating the peacetime-wartime build and creating a seamless continuing construct, enables better intelligence and builds capabilities suited to the realities of conflict.

- Establish a National Cyber Command (NCC) for efficient cyberspace management to develop capabilities and work to evolve towards pioneering full spectrum information superiority operations.

- Coordinate, synergise and centralise all existing military and civil cyber efforts of Defence Cyber Agency (DCyA), Signal Intelligence (SI), Military Intelligence (MI), Electronic Intelligence, HUMINT, Army Cyber Group, Additional Directorate General Strategic Communication, Defence Research and Development Organisation (DRDO), National Technical Research Organisation, Research and Analysis Wing, National Investigation Agency and operational security under NCC for a comprehensive threat analysis and coordinated response.

- Upgrade of DCyA to a full-fledged Defence Cyber Command with requisite formations at the regional level.

- Aim towards active and AI-enabled Cyber Defence and Deception at Cyber Military Command and Corps, whereas CNE and CNO are to be controlled, coordinated and executed as a centralised function under DCyA and NCC due to reasons as explained above.

- Integrate cyber power with EW, satellites and space creating exponential capabilities in generating desired effects. The defence forces coordinate for synergised application of cyber in the digital battlefield by initiating and developing Cyber and Electromagnetic Activities capabilities.[11]

Training and Human Resources (HR)

- Establish national-level programmes, state and national-level hackathons and conduct Black/Red HAT conferences/ seminars in identifying young talent and nurturing the same for a secured career and cadre.

- Outsource national and international training of selected defence and civil candidates for incorporating system integration of cyber with EW, information warfare and kinetic energy assets.

- Improve HR policies since CNE/CNO operations have no defined working hours (365 days, 24/7), thus, compassionate ground and marital discord postings should not be allowed in such units.

- Postings to such units be considered as probations and finalised only if the trainability and usability of the individuals are confirmed by the Cyber Unit.

- Make provisions for extended tenures and grant adequately exercised/long course/posting profile waivers for handpicked manpower to be incorporated in policies.

- Establish world-class training facilities along with industry and academia with highly qualified faculty.[12] Indian Institute of Technology to be made centre of excellence and collaborate with Centre for Intelligence Research and Analyses, DRDO for identification and development of vulnerabilities and their weaponisation for central cyber agencies.

- Establish an independent tri-service institute 'Military Institute of Information Superiority' for cyber training of all SI, MI, Cyber Commands/DCyA etc. This shall accrue a common understanding of cyber requirements under a single roof and achieve synchronised development of strategy also enabling talent spotting and cadre management.

Conclusion

With the advent of the digital platform as the 5th dimension of warfare, with the capability to reach and affect the global population instantaneously in real-time, there is an urgent need to develop self-reliance in establishing credible cyber deterrence and defence competency. The dimension is presently dominated by Western developed countries due to the inherent lead in establishing a global network of systems, services and applications due to the subjugation of Global South countries during the colonial era. Now, Bharat is at the cusp of dominating this dimension with the world's largest young demographic profile with an acumen pioneering in the field of ICT world across the world. Bharat needs to take the initiative and set in motion various checks and balances to be *Atmanirbhar*, master the trade and lead the globe in the art of information superiority.

Endnotes

[1] Connected devices will be 3x the global population by 2023, Cisco says - RCR Wireless News

[2] US Joint Chiefs of Staff, Joint Publication 3-13 'Information Operations' dated 27 Nov 2012.

[3] "How am I in this war?": New Musk biography offers fresh details about the billionaire's Ukraine dilemma.
https://edition.cnn.com.

[4] "The most powerful Indian technologists in Silicon Valley", The Guardian, 2014.
https://www.theguardian.com/technology/2014/apr/11/powerful-indians-silicon-valley.

[5] A timeline of Elon Musk's takeover of Twitter.
https://www.nbcnews.com.

[6] India Becomes a Global AI Powerhouse with 13.2 Million Developers on GitHub.
https://analyticsindiamag.com.

[7] Namrata Goswami, "The Reorganization of China's Space Force: Strategic and Organizational Implications", The Diplomat, 03 May 2024.
https://thediplomat.com/2024/05/the-reorganization-of-chinas-space-force-strategic-and-organizational-implications/.

[8] Credible Cyber Deterrence in Armed Forces of India, A task force study by Vivekananda International Foundation Mar 2019.

[9] "Threatscape Segmentation: Network Invigilation for Realizing Vulnerable Assets using Neutral Analytics (Nirvana) to Mitigate Zero Day Attacks" by Lt Col Vivek Bardia, DEFCON India 2019.

[10] "Credible Cyber Deterrence in Armed Forces of India", A task force study by Vivekananda International Foundation Mar 2019.

[11] "Credible Cyber Deterrence in Armed Forces of India", A task force study by Vivekananda International Foundation Mar 2019.

[12] "Credible Cyber Deterrence in Armed Forces of India", A task force study by Vivekananda International Foundation Mar 2019.