Cyber Warfare:
Protecting the Soldier

S KULSHRESTHA

> *The machine has presented us with a central nervous system, protected with no spinal vertebrae, lying almost naked for the cutting. If, for one reason or another, the severance is made, we face a terrifying, perhaps mortal crisis…. Day by day the complexity, and, hence, the potential danger, accelerates; materials and structures ceaselessly and silently deteriorate.*
>
> *Stuart Chase, in Men and Machines, 1929*

The warfare domains have traditionally included those which have geographic and topographic war-fighting constraints, for example, the land, sea, and air (now aerospace) domains. However, in cyber warfare, the physical domains are no longer relevant since the domain has changed to the all-encompassing global electromagnetic spectrum. There is a need, therefore, to look for the definition of the cyber space in which a modern soldier is required to operate.

The US Department of Defence defines cyber space as "a 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]

Kuehl has defined it as[2] "an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via inter-connected information and communication technology-based systems and their associated infrastructures."

The above definitions draw upon the interrelated effects of the physical, informational, and cognitive domains. These together comprise the physical platforms, systems and infrastructure that provide global connectivity to interconnect information systems, networks, and human users; the massive amounts of information that can be digitally and electronically shared; and the impact on human behaviour and decision-making when faced with the deluge of information.[3]

Some characteristics of cyber space are that it exists and functions within the natural Electromagnetic Spectrum (EMS); it exists due to man-made technologies; it can be replicated; and it is far more economical to operate and utilise than other domains. These lead to a more encompassing definition of cyber space,[4] "It is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies".

Cyber space has been preferred by nations, criminals and hackers for cyber attacks across the globe due to the fact that its usage is becoming the backbone of the society; the current systems do not have adequate protection and predictive intrusion detection systems[5]; it is very fast, its reach is worldwide, and it provides anonymity. The increasing usage of digital sensing, and software-based control in critical infrastructure, and dependence upon the communication network for movement of network-based data has made cyber security a national security problem. Cyber security can be defined[6] as, "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation".

Based upon the above, military cyber power can be defined[7] as "the application of operational concepts, strategies, and functions that employ the tools of cyber space to accomplish military objectives and missions".

Cyber Threat Assessment: China

The establishment of the People's Liberation Army's (PLA) Cyber Space Strategic Intelligence Research Centre in June 2014 to "provide strong support in obtaining high-quality intelligence research findings and help China gain advantage in national information security" indicates the focus of the PLA on cyber space[8]. The Strategic Support Force (SSF) of China is a military theatre-grade organisation

Cyber Space is preferred for cyber-attacks as its usage is becoming the backbone of society.

responsible for the space, cyber, and electronic warfare missions of the PLA and strategic-level information support for joint operations. The SSF is more or less the information warfare branch of the People's Liberation Army. It is understood that it will be composed of three separate forces: space troops (recognition and navigation satellites), cyber troops (offensive and defensive hacking), and electronic warfare forces (jamming and disrupting radars and communications).[9] As per Rear Admiral Yin Zhuo, its main task will be ensuring the military's local advantages in aerospace, space, cyber, and electromagnetic battlefields through operations such as target tracking and reconnaissance, satellite navigation, and attack and defence in the cyber and electromagnetic spaces – the underlying goal of which should be attaining victory in future wars. Further, the SSF will assume responsibilities in defending the civilian infrastructure to increase the security of China's financial institutions as well as people's daily lives in general[10]. It implies that the SSF will be responsible for all aspects of information warfare, including intelligence, technical reconnaissance, cyber warfare, and electronic warfare. This is in line with China's strategic thinking, which sees paralysing and sabotaging the enemy's operational and command systems as a key to achieving dominance in all other domains: land, sea, and air[11].

Desmond Ball has brought out that PLA Information Warfare (IW) units have reportedly developed and tested 'detailed procedures' for internet warfare, including software for network scanning, obtaining passwords and breaking codes, and stealing data; information-paralysing software, information-blocking software, information-deception software and other malware; and software for effecting counter-measures. These procedures have been tested during simulated cyber attacks against Taiwan, India, Japan and South Korea. The PLA has reportedly established at least twelve facilities for Integrated Network Electronic Warfare (INEW) training at unit levels in computer network attack and defence operations, jamming and other forms of electronic warfare, and other IW activities. The facility is supposedly located at Zhurihe in the Beijing Military Region[12].

It is understood that Chinese hackers have been able to crash selected web servers, penetrate websites and deface them, erase data from them, post on them, and have developed various viruses/Trojan Horse programmes for spreading/inserting by e-mails to disable/steal information from targeted computer systems. However, there is no evidence yet that these hackers would be able to penetrate highly secure networks/command and control or weapon system networks to copy or manipulate critical data. Currently, China's extensive cyber warfare capabilities are very good for simple attacks but not for sustained cyber warfare. As a result, the PLA may seek to use its cyber warfare capabilities to collect data for intelligence and cyber attack purposes; to constrain an adversary's actions by targeting network-based logistics, communications, and commercial activities; or to serve as a force multiplier when coupled with kinetic attacks during times of crisis or conflict[13].

Future soldier will be subjected to direct and indirect cyber-attacks in a complex battle environment.

Military Cyber Vulnerabilities

The Future Soldier Vision (FSV) design for the UK as unveiled by the UK Ministry of Defence (MoD) includes[14]:

- Head sub-system concept incorporating hearing protection, lightweight sensors for information sharing and an integrated power supply.
- Torso sub-system concept of segmented armour that can be customised to the user or situation with integrated connectors and power supply.
- Smart watch style wearable communications concept which incorporates sensors to record the user's biometric data.
- Smart glasses concept which includes a heads-up display, integrated camera and bone conducting headphones to increase situational awareness without compromising hearing.
- A robust personal role computer concept enabling better information sharing and communications between personnel.
- Ergonomically designed and customisable, the weapon concept will allow targeting information to be shared between soldiers and their units.
- Further, the FSV is designed to work as an integrated system, with survivability, enhanced situational awareness and network capability. Protection technology, a network of sensors for information sharing and power and data connectors will also all be built-in.

At the 2017 Association of the United States Army annual meeting (AUSA 2017), the US Army Research, Development, and Engineering Command (RDECOM) presented a concept for the US Army's future soldier of the 2030 which also promised everything from powered exoskeletons, to futuristic optics, to individual network capability[15].

The modernisation programme for the infantry in India began with the F-INSAS (Future Infantry Soldier as a System), but it has now evolved into two separate programmes: arming the infantry with better offensive and defensive gear and the battlefield management system. The system is technology based with sensors, laser range finders, cameras, etc. The system will merge the information to give the soldier a real-time picture of the battlefield. The tactical level communication will take place over secure radio networks, and command level communication would be carried over Indian satellites. Each soldier will have a personal Global Positioning System (GPS) device and will be able to see the position of other soldiers via a helmet mounted display[16].

As can be envisioned from the FSV above, the future soldier would be operating in an environment where he would be subjected to direct and indirect cyber attacks by the adversary since the FSV is designed around the core concept of network-centric warfare. In addition to the FSV, the complete architecture of modern warfare revolves around network-centricity which itself is vulnerable to cyber attack.

Military Systems

The military cyber space domain under which its systems operate comprises two major types of networks, namely, an open network which relies on data-sharing, situational awareness and team work, whereas the other utilises secure networks which depend upon speed, reliability and data integrity. The military communications utilise various types of modes for example, the global communications systems, military controlled commercial networks, and highly secure networks for target-shooter systems.

Complex military Command, Control, Communications, Computers, Intelligence (C4I) systems are increasingly relying on sophisticated software and communication systems and, hence, they remain lucrative targets for hackers and adversary states. Next come the weapon systems which use software like aircraft, warships and military special vehicles. Thereafter, the communication nodes, wide area networks, logistics and GPS feeds, etc. Ingress into a system using software can be made by physical means through inputs to the system for example, like spare ports, by installing malware, or installing clandestine wireless devices. Indirect ingress can be made through connectivity ports for example, through the internet, or through a connection leading from other computers, or indirectly accessing the device from a distance using operating software vulnerabilities. In the case of the military, both these methods of attack can be guarded against effectively but not absolutely.

The widespread usage of Commercial-Off-The-Shelf (COTS) or open-source systems for military uses has increased the vulnerability to cyber attack, and their use should be guided by policies that assure the military of obviating the risks and by carrying out a risk and cost benefit study.[17] Standardisation has reduced costs, but it exposes a large number of similar products through the exploitation of common vulnerabilities. Trojan horses could be introduced in the process of developing or maintaining the software. Vulnerabilities could be deliberately planted in a device or software programme. By and large, critical military systems are carefully designed and operated and are expected to remain safe during cyber attacks.

The cyber space interlays and overlays with the civilian and military cyber domains, therefore, even though military defences at local level can be strengthened, using physical access controls, password regimes, complex logging procedures and biometrics, isolation, human interfaces for critical equipment operations, etc, it is an effort at the policy level which has to be put in place by the government so that the cyber attack does not debilitate national security.

Policy Level Efforts

The US Department of Defence (DoD) has three primary cyber missions: defend DoD networks, systems, and information; defend the nation against cyber attacks of significant consequence; and support operational and contingency plans.

The US DoD has set five strategic goals for its cyber space missions[18]:

- Build and maintain ready forces and capabilities to conduct cyber space operations: This strategy sets specific objectives for the DoD with regard to manning, training, and equipping its forces and personnel over the next five years and beyond.
- Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions: DoD must take steps to identify, prioritise, and defend its most important networks and data so that it can carry out its missions effectively. DoD must also plan and exercise to operate within a degraded and disrupted cyber environment in the event that an attack on the DoD's networks and data succeeds, or if aspects of the critical infrastructure on which the DoD relies for its operational and contingency plans are disrupted.
- Be prepared to defend the US homeland and US vital interests against disruptive or destructive cyber attacks of significant consequence: The D0D must work with its inter-agency partners, the private sector, and

allied and partner nations to deter and, if necessary, defeat a cyber attack of significant consequence on the US homeland and US interests.

- Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages: During heightened tensions or outright hostilities, the DoD must be able to provide the President with a wide range of options for managing conflict escalation. If directed, the DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities.
- Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability: all three of the DoD's cyber missions require close collaboration with foreign allies and partners. In its international cyber engagement, the DoD seeks to build partnership capacity in cyber security and cyber defence, and to deepen operational partnerships where appropriate.

Way Ahead

It would be utopian to expect an integrated military cyber space infrastructure which can fulfil all the requirements of open and closed networks of the military to cater to its multifarious requirements of data sharing and weapon-shooter-target engagements. Further, expecting it to be vulnerability-proof, having infinite bandwidth, reliable, survivable and upgradable, virtually amounts to asking for the moon. However, under the prevalent technology regime, a pragmatic structure can be provided with sufficient redundancy to enable it to withstand cyber attacks and carry out assigned tasks during the period of the conflict. Two major adversaries, the US and China, have well defined cyber security policies in place which offer India a workable platform for tailoring its own policy. The Government of India is planning to create a new tri-Service agency for cyber warfare. The Defence Cyber Agency will work in coordination with the National Cyber Security Advisor. It will have more than 1,000 experts who will be distributed into a number of formations of the Army, Navy and Air Force. According to reports, the new Defence Cyber Agency will have both offensive and defensive capacity[19]. It would be the exhaustive implementation of this policy, as and when it materialises, which would protect the soldier during a cyber war.

Rear Admiral **Dr S Kulshrestha** (Retd), is an avid contributor to CLAWS. The views expressed are personal.

Notes

1. Joint Chiefs of Staff, Joint Publication 1-02, Washington DC, US Department of Defense, November 08, 2010; as amended through February15, 2016. https://fas.org/irp/doddir/dod/jp1_02.pdf. Accessed January 01, 2018).
2. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington D.C., National Defense University Press, Potomac Books, 2009). http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-02.pdf. Accessed on January 01, 2018.
3. Ibid.
4. Ibid.
5. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Ecco, 2010), pp. 103-149.
6. Ibid.
7. Elihu Zimet and Charles L. Barry, "Military Service Cyber Overview" in Larry K. Wentz, Charles L. Barry, Stuart H. Starr, eds., *Military Perspectives on Cyberpower* (Washington, DC: Center for Technology and National Security Policy at the National Defence University, July 2009). https://www.hsdl.org/?view&did=32100. Accessed on January 02, 2018.
8. Jianing Yao, "PLA Cyberspace Strategic Intelligence Research Center Founded," *China's Military*, June 30, 2014. http://eng.chinamil.com.cn/news-channels/china-military-news/2014-06/30/content_6025789.htm. Accessed on January 03, 2018.
9. Mikk Raud, *China and Cyber: Attitudes, Strategies, Organization* (Tallin: The NATO Cooperative Cyber Defence Centre of Excellence, 2016). https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf. Accessed on January 01, 2018.
10. John Costello, "The Strategic Support Force: China's Information Warfare Service," *The Jamestown Foundation*, February 08, 2016. http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=45075&cHash=9758054639ab2cb6bc7868e96736b6cb#.V6RA_Lt95aQ>. Accessed on August 23, 2016. Accessed on January 01, 2018.
11. Ibid.
12. Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges*, Vol. 7, No. 2, Winter 2011, pp. 81-103. https://indianstrategicknowledgeonline.com/web/china%20cyber.pdf. Accessed on January 01, 2018.
13. Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017. https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF. Accessed on January 02, 2018.
14. Ministry of Defence, UK, Defence Science and Technology Laboratory, and The Rt Hon Sir Michael Fallon MP, "MOD Unveils Futuristic Uniform Design," September 16, 2015. https://www.gov.uk/government/news/mod-unveils-futuristic-uniform-design. Accessed on January 02, 2018.
15. Nathaniel F., "SOLDIER OF THE FUTURE," Concept Displayed by US Army at (AUSA 2017). The Firearm Blog, October 30, 2017. http://www.thefirearmblog.com/blog/2017/10/30/soldier-future-concept-displayed-us-army-ausa-2017/. Accessed on January 01, 2018.
16. Abhishek Saksena, "Indian Army's Future Infantry Soldiers to get Lethal Weapons and Better Protection," *India Times*, January 18, 2017. https://www.indiatimes.com/culture/

who-we-are/indian-army-s-future-infantry-soldiers-to-get-lethal-weapons-and-better-protection-269775.html. Accessed on January 03, 2018.

17. Howard F. Lipson, Nancy R. Mead, and Andrew P. Moore, "Can We Ever Build Survivable Systems from COTS Components?" CMU/SEI–2001–TN–030 (Pittsburgh: Carnegie Mellon University, Software Engineering Institute, December 2001). http://repository.cmu.edu/cgi/viewcontent.cgi?article=1630&context=sei. Accessed on January 01, 2018.
18. "The DoD Cyber Strategy 2015," https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. Accessed on January 05, 2018.
19. "India is Quietly Preparing a Cyber Warfare Unit to Fight a New Kind of Enemy," https://economictimes.indiatimes.com/news/defence/india-is-quietly-preparing-a-cyber-warfare-unit-to-fight-a-new-kind-of-enemy/articleshow/61141277.cms. Accessed on January 05, 2018.