China's Cyber Warfare Capabilities

Brigadier Saurabh Tewari[@]

Abstract

The potency and overwhelming lethal effects of cyber warfare have outpaced the technological development in conventional military weapons space, changing the very character of future wars, and the role of cyber warfare in them. Worldwide cyber warfare is now being acknowledged as the fifth dimension of warfare.

In the last decade or so there has been consistency in reports of cyber intrusions in India from China. Important Indian targets include ministries, embassies, industrial houses, defence establishments, apart from sensitive government offices. No Indian cyber intrusion investigation reports are available in the open domain; however, investigation reports of major cyber breaches world over by foreign investigators do exist, wherein India is mentioned as one of the victims, with intrusions attributed to China.

China and Pakistan are known to be developing cyber warfare capability to deter a physically and technologically superior military adversary. India needs to be aware and conscious of these threats, and needs to develop counter capabilities. In the last decade. China has made considerable progress in developing cyber warfare capabilities in terms of revising its policies, restructuring organisations, building human expertise, and raising new establishments.

This article analyses Chinese cyber warfare strategy and capabilities and its impact on India.

[@]**Brigadier Saurabh Tewari** is B Tech in Electronics and Telecommunications and M Tech in Optical Communications. He has served in insurgency affected areas, Siachen Glacier, Ladakh and Sri Lanka. He holds PG diploma in management and diploma in Cyber Law.

Journal of the United Service Institution of India, Vol. CXLIX, No. 616, April-June 2019.

Global Cyber Warfare Trends

Although one saw glimpses of cyber and electronic warfare in the Gulf War, there has been a major rise in use of cyber warfare by nation states over the last decade or so, as elucidated below:-

(a) In 2007, operation "Orchid" was carried out by the Israeli Air Force to destroy Syrian nuclear facilities near the border, in which Israel resorted to cyber warfare to blind the Syrian air defence system (radars) deployed along the Syrian-Israel border. Taking it's advantage the Israeli air force fighter aircraft bombed the nuclear facility without being detected by Syrian radars.[1,2]

(b) In 2010, the stuxnet virus destroyed a major portion of Iranian nuclear facility. This incident was globally assessed as a joint effort of Israel and the USA.[3]

(c) In 2012, there was a major power grid failure in northern India, and reports indicate that the same could be attributable to hacking of the Supervisory Control and Data Acquisition System (SCADA) by a China-Pakistan nexus.[4]

(d) In 2014/15, during Russian - Ukraine conflicts, Russians resorted to blanking of Ukraine military communication systems, thereby forcing them to use the cellular network, which enabled their location fixing, and easing their neutralisation.[5,6]

(e) In 2016, the deadly ransom-ware virus Wannacry adversely effected individual and organisational networks across the globe.

These events go to show that cyber warfare is now the preferred tool, being non-contact, shrouded in obscurity, and low cost, but having an infinite reach.

Cyber Warfare Incidents against India

Cyber incidents against India have been occurring at regular intervals, especially in the last decade. This has been acknowledged at the highest levels like the former National Security Advisor (NSA) of India, MK Narayanan.[7] Recently, a report by US Cyber Security Company, called 'FireEye', said that China has been spying on Indian government and business for more than a decade

without India being aware of it, and there is more to come.[8] The consistency of incidents indicate a dedicated India-targeted espionage system purportedly originating in China. Summary of some activities is given below:-

(a) 2009: National Informatics Centre (NIC) servers breached.

(b) 2012: Ministry of Home Affairs (MHA), Ministry of External Affairs (MEA) intruded.[9]

(c) 2012: Northern India Power grid crashed.[10]

(d) 2013: Defence Research and Development Organistaion (DRDO), Prime Minister's Office (PMO) website hacked.[11]

(e) 2014: Bharat Sanchar Nigam Limited (BSNL) website hacked.[12]

(f) 2015: Indian Space Research Organisation (ISRO) webpage defaced.[13]

(g) On 23 May 2017, an Indian Air Force Sukhoi 30 fighter aircraft was downed, purportedly by a cyber attack from China.[14]

Understanding our vulnerabilities and China's cyber capabilities will play a major role in arriving at appropriate response to accredit cyber attacks to China and undertake countermeasures. Own vulnerabilities are two-fold. Firstly, there is a lack of effective cyber security environment, integration amongst organisations and lack of offensive capability. Secondly, vast proliferation of Chinese computer and telecommunication hardware, as well as mobile phones have increased vulnerabilities to a great extent.

Chinese Cyber Warfare Capabilities

In April 1997, a 100-member elite corps was set up by the Central Military Commission (CMC) to devise ways of hacking into American and other western countries computer systems. Since then, China has been making steady progress in acquiring cyber warfare capabilities in terms of organisations, policies and expertise. In 2015, People's Liberation Army (PLA) decided to raise Strategic Support Force which is being touted as the fifth Service and not just a branch of PLA.[15,16]

China uses the term "Integrated Network Electronic Warfare" (INEW) to describe an integrated approach to information warfare operations and includes electronic warfare (EW), computer network warfare and psychological operations.[17] Salient aspects of Chinese strategy on cyber space are given below:-

(a) **Global Superpower.** China aims to become global internet superpower and have an impregnable cyber security system by 2025.[18] Apropos, it is reasonable to assume that China would develop its cyber warfare capabilities in equal measure.

(b) **Whole of Nation Approach.** China has *"Whole of Nation"* approach **for** conducting cyber war, to include patriotic hackers and university students as cyber warriors in conjunction with the PLA.[19]

(c) **First Option.** The PLA sees cyber warfare as a first-strike option to preclude the requirement of conventional military operations, and not as a force multiplier to conventional operations.[20]

(d) **Strategic / Space Cyber War.** China has elevated cyber warfare to strategic level by adding cyber attacks on satellites or space warfare, to its offensive operations.[21]

(e) **Concurrency.** It is logical to assume that PLA intends to conduct concurrent operations in all five domains viz. land, sea, air, space and cyber.

(f) **Cyber Espionage.** China is involved in continuous cyber reconnaissance to identify weak spots and glean information which can be exploited during war.

(g) **Crippling the Critical Infrastructure.** Target information infrastructure of critical services like financial institutions, banking, electrical, water, sewage, railway and telecommunication networks.

(h) Proliferate Chinese computers / laptops, modems and telecommunication hardware in enemy country networks (embedded with virus, trojans, malware), which can glean information on regular basis, and may be exploited later during war to cripple the nation.

Important Cyber Organisations

The major cyber organisations of China are:-

(a) **PLA 3rd Department.** 3rd Department is responsible for Signal Intelligence (SIGINT), Computer Network Defence (CND) and Computer Network Exploitation (CNE).[22,23]

(b) **PLA 4th Department.** 4th Department is responsible for Electronic Warfare (EW), Computer Network Attack (CNA) and Integrated Network Electronic Warfare (INEW).[24]

(c) **IW Militia Units.** Militia units were established by the PLA in 2002 within commercial organisations.[25]

(d) **Strategic Support Force (SSF).** China created a new force called the SSF in 2015 which is likely to integrate intelligence, communications, electronic warfare with cyber warfare to create an integrated information warfare force.

(e) **Non State Actors –** This comprises:-

(i) **State Backed Hackers.** Keeping with the concept of 'whole of nation' approach, university students and patriotic hacker groups are facilitated by the PLA and transformed into legitimate cyber warfare units. Hackers are recruited under the guise of software engineers and security experts. China is purportedly maintaining approximately 30,000 citizens and 250 Patriotic Hacker groups.

(ii) **Telecommunication Enterprises.** Civil telecommunication companies are part of China's cyber espionage system. Firms like Huawei, and ZTE are closely associated with the government and receive preferential funding for Research and Development and predatory trading.

Implications for India

(a) **Cyber Environment.** The cyber environment in India is very discouraging, to say the least. Penetration testing by own agencies have divulged that Indian networks/computers are flooded with virus, trojans etc. Most of the critical hardware like routers could be easily penetrated. This includes hardware of important and critical organisations like the DRDO, National

Thermal Power Corporation (NTPC), police, Public Works Department (PWD), finance, space, ministries etc.

(b) **Chinese Hardware.** Chinese firms like ZTE and Huawei have been underbidding in tendering process in India (and elsewhere, eg USA) and thereby, becoming the L1 (lowest) bidder.[26,27] To do this, they probably get the financial support from State owned banks in China. As a result, a number of computers and telecommunication hardware in Indian telecommunication networks, government departments, railway network, power network etc. are of Chinese origin and are (in all likely-hood) infested with virus, worms and trojans. It is almost a foregone conclusion that China is collecting all the critical information about our networks/ systems which may be used to disrupt them at a critical time. Further, classified information is also being stolen from computers.

(c) **Commercial Off-The-Shelf (COTS) Microchips**. China is the major source of silicon integrated microchips (being used in all electronic devices) for all manufacturers across the globe, including American and European brands.[28,29] Possibility of undesired alterations in these integrated circuits cannot be ruled out. Consequently, China's intelligence collection and system vulnerability identification would give the PLA a tremendous advantage in a confrontation situation with India.

(d) **Threat to Critical Infrastructure.** Way back in August 2012, when the northern power grid failed, cyber analysts suspected "Pak-China" nexus for the failure. In 2015, in a letter to the NSA, Ajit Doval, Indian Electronics and Electricals Manufacturers' Association (IEEMA)[30], asked for a complete ban on Chinese equipment in the Indian power sector citing security concerns. According to IEEMA's database, in the last decade, India's import of electrical equipment has increased considerably and in order to make power distribution network efficient, many cities in India have awarded the contract to deploy Supervisory Control and Data Acquisition system (SCADA) to Chinese firms which pose a danger to the power infrastructure. Similarly, there is a grave threat to other critical infrastructure like telecommunication, railways,

irrigation etc. which are dependent on telecommunication / IT hardware and SCADA systems.

(e) **Digital India.** The digital India focus of present government is a cause for concern as digital economy is being pushed without requisite cyber safety measures being in place. The recent news about availability of personal AADHAAR data of Indian citizens at a mere Rs 500 is shocking to say the least, and should be a major wake-up call for the government.

(f) **Lack of Integration between Various Agencies.** India has various organisations dealing with cyber issues like the National Technical Research Organisation (NTRO), National Critical Information Infrastructure Protection Centre (NCIIPC), National Cyber Coordination Centre (NCCC), Tri Service Cyber Command for the Armed Forces (proposed) etc. However; they are not integrated with each other and operate independently. There is a need to have a single policy level agency and a single execution level agency, which can coordinate at national level, so as to derive maximum dividends out of the efforts being put in.

(g) **Development of HR.** The total strength of cyber security experts deployed in various government agencies of the government is mere 550 compared to 1 lac+ in China, 91,000 in USA and 7000 in Russia.[31] There is thus a dire need to develop and hire cyber security experts by the government and exploit their talent to protect critical information infrastructure as well as acquire cyber offensive capabilities.

(h) **No Research Institution.** China has a number of cyber security academies to train cyber experts. India too should establish such state sponsored academic institutions.

Conclusion

Indian is moving fast on the road to digital India, including digital economy, in a big way. If it does not want to be surprised, India should prepare for futuristic war in cyber domain. With society becoming increasingly dependent on automation and computers, and concepts like Internet of Things (IoT) knocking at our doors, we will become vulnerable to information warfare attacks.

Further, as time progresses, China will develop greater expertise and sophistication in its understanding of information warfare techniques. Unless India takes concrete steps to strengthen its cyber security posture and develop cyber warfare capabilities to match that of China, we may be facing a grim situation, sooner than later.

Endnotes

[1] http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html, Accessed 11 Nov 2018

[2] https://www.timesofisrael.com/israel-uses-17-tons-of-explosives-to-destroy-syrian-reactor/, Accessed 11 Nov 2018

[3] http://large.stanford.edu/courses/2015/ph241/holloway1/, Accessed 11 Nov 2018

[4] https://www.oneindia.com/2012/08/22/china-s-hand-in-india-s-power-blackout-1057676.html, Accessed 11 Nov 2018

[5] Cyber and Information warfare in the Ukrainian conflict, Marie Baezner & Patrice Robin, Center for Security Studies (CSS), ETH Zürich (https://www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict), Accessed 11 Nov 2018

[6] https://www.wired.com/story/russian-hackers-attack-ukraine, Accessed 11 Nov 2018

[7] Sharma Deepak, 2011, *China's Cyber Warfare Capability and India's Concerns,* Institute for Defence Studies and Analyses, New Delhi (https://idsa.in/system/files/jds_5_2_dsharma.pdf) Accessed 22 Aug 2018

[8] https://entrackr.com/2017/12/fireeye-chinese-hackers-target-india-2018/, Accessed 22 Aug 2018

[9] http://www.indiandefencereview.com/spotlights/acupuncture-warfare-chinas-cyberwar-doctrine-and-implications-for-india/, Accessed 28 Aug 2018

[10] https://www.oneindia.com/2012/08/22/china-s-hand-in-india-s-power-blackout-1057676.html, Accessed 21 Sep 2018

[11] http://www.thehindu.com/news/national/drdo-website-hacked/article4051758.ece, Accessed 21 Sep 2018

[12] https://www.thehindubusinessline.com/info-tech/bsnl-site-hacked/article7386407.ece, Accessed 21 Sep 2018

[13] http://www.thehindu.com/news/national/isros-commercial-arm-antrix-website-hacked/article7413823.ece, Accessed 28 Sep 2018

[14] https://www.cybersecurity-insiders.com/china-cyber-attacks-indian-sukhoi-30-jet-fighters/, Accessed 13 Nov 2018

[15] https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military. Accessed on 21 Nov 2018

[16] https://www.rand.org/pubs/research_reports/RR2058.html. Accessed on 21 Nov 2018

[17] Sharma Deepak, 2010, *Integrated Network Electronic Warfare: China's New Concept of Information Warfare,* Journal of Defence Studies: Vol 4. No 2, Apr 2010, published by Institute for Defence Studies and Analyses, New Delhi (https://idsa.in/jds/4_2_2010_ChinasNewConceptofInformationWarfare_dsharma) Accessed 22 Aug 2018

[18] http://www.scmp.com/news/china/policies-politics/article/1995936/china-aims-become-internet-cyberpower-2020, Accessed 10 Oct 2018

[19] Klimburg Alexander, 2011, *The Whole of Nation in Cyber-power*, Georgetown Journal of International Affairs, pp 171-179 (https://www.jstor.org/stable/43133826?newaccount=true&read-now=1&seq=1#metadata_info_tab_contents) Accessed 08 Oct 2018

[20] Sharma Deepak, n 7

[21] http://www.indiandefencereview.com/spotlights/acupuncture-warfare-chinas-cyberwar-doctrine-and-implications-for-india/, Accessed 20 Oct 2018

[22] https://www.globalsecurity.org/intell/world/china/pla-dept_3.htm, Accessed 20 Oct 2018

[23] The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure, Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, 2011, The Project 2049 Institute (http://goodtimesweb.org/surveillance/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf) Accessed 20 Nov 2018

[24] Sharma Deepak, n 7

[25] Sharma Deepak, n 7

[26] https://www.ft.com/content/42bd9a40-5900-11de-80b3-00144feabdc0, Accessed 20 Nov 2018

[27] http://indianexpress.com/article/world/china-must-cease-predatory-trade-practices-us-4903350/, Accessed 20 Nov 2018

[28] http://www.information-age.com/security-backdoor-found-in-china-made-us-military-chip-2105468/, Accessed 20 Nov 2018

[29] https://www.military.com/defensetech/2012/05/30/smoking-gun-proof-that-military-chips-from-china-are-infected, Accessed 20 Nov 2018

[30] http://www.thehindu.com/business/Industry/china-poses-security-threat-in-power-sector-trade-body/article17452568.ece, Accessed 20 Nov 2018

[31] http://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber-security-experts/article4827644.ece, Accessed 20 Nov 2018