National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

CYBER WARFARE AND CHALLENGES FOR PAKISTAN

Major Jawad Yaqub

JCSP 46

Service Paper

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 46

Étude militaire

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46
2019 – 2020

SERVICE PAPER - ÉTUDE MILITAIRE

CYBER WARFARE AND CHALLENGES FOR PAKISTAN

Major Jawad Yaqub

Word Count : 2,393

Nombre de mots : 2.393

CYBER WARFARE AND CHALLENGES FOR PAKISTAN

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.

– Giulio Douhet, The Command of Air

AIM

1. The aim of this paper is to examine cyber aspects of emerging hybrid threat against Pakistan, specially from our arch adversary, highlighting vulnerabilities with a view to propose response measures to counter the cyber threat thus posed. The paper is intended to bring in focus the application of cyber tool in future India and Pakistan *(Indo-Pak)* scenario, existing gaps and a suggested course of action for Pakistan. More consideration has been kept on the national level response in structural domain and still there is a need to deeply analyse the functional shortcomings specially at lower level.

INTRODUCTION

2. Cyber conflicts are a new normal to the modern hybrid warfare, where nations unleash their digital dominance upon each other. [1] It is an extremely effective and in-expensive tool of warfare which has replaced soldiers and fleets with few strokes of keys, still equally capable of bringing widespread and wide-ranging destruction upon enemy. Many countries have adopted it as a principal weapon against their adversaries. Pakistan too, is extremely vulnerable to cyber-attacks, specially by her arch-rival India which has embarked hybrid war upon it ever since independence.[2]

[1] Brigadier Ahsan Mehmood Khan, " Hybrid Warfare: A Conceptual Perspective", Hilal, 1 Feb 2018

[2] Transcript of second confessional statement of Commander Kulbushan Sudhir Jhadav. Inter Services Public Relations press release - 322/ 2017. “Research and Analysis Wing (RAW) was sponsoring the setting up of modern website, being run through Nepal on the Cyber world which was luring people from within Pakistan for various activities to be carried out in the future”.

3. Due to widespread induction of computer technology in every field of life, cyber-attacks have the potential to literally effect all pillars of national power. Most of the modern military gadgetry, i.e., weapon systems, surveillance and targeting systems are embedded with microprocessors and chips which make them extremely vulnerable to cyber-attacks. Our adversary with clear edge in information technology is capable enough to exploit these weaknesses. Therefore, it is imperative to look into the existing voids in relation to the threat spectrum, so as to enhance our cyber capabilities and effectively deter these emerging challenges. This paper will first cover the context of cyber war in future Indo-Pak conflicts, followed by threat analysis and likely target areas, ending up with suggesting a future course of action.

DISCUSSION

Nature of Future Indo-Pak Conflicts

4. Pakistan and India have fought three major wars since 1947. There has been a few military stand-offs and escalations but no conventional war after 1971. The nuclear capability of both countries has greatly reduced the space for conventional conflicts and given way to limited wars. Although South Asia is considered a nuclear flashpoint, but in fact nuclear factor has deterred the full-scale war rather than fighting it.[3] Moreover, none of the side has that edge in military capability which can win a war for it. Therefore, it would be safe to assume that future war would be short with limited objectives. Given the constraints, belligerents are more likely to exploit information/ digital domain to degrade the potential and break the will of enemy to fight.

[3] Stephen Philip Cohen, "Nuclear Weapons and Nuclear War in South Asia: An Unknowable Future", A Paper Presented to the United Nations University Conference on South Asia, Tokyo, Japan, May 2002.

5. In this context cyber war figures out to be a very handy weapon, which would not only enable engaging wide set of targets, but doing so while remaining well below the conventional war threshold. It's low cost, low risk and covert nature makes it extremely relevant to Indo-Pak scenario.

Cyber Threat Perception

6. Indian Standing in IT World. India is considered to be an IT giant of tomorrow with its ever-flourishing software and hardware industry.[4] Its computer software technology gives a strategic edge over Pakistan. The Indian software exports turn out to be over 100 billion USD which speaks volumes of its expertise in this field and the future potential.[5] Software services contribute 7.7% of country's GDP. Nonetheless, India is considered IT giant of tomorrow. All these capabilities if harnessed and exploited, can pose a formidable challenge for Pakistan. General V.P. Malik ex Indian Army Chief, insistently stressed upon the message that "Cyber war is to the 21st century what Blitzkrieg was to the 20th". He took series of measures and initiated modernization plans in this regard.[6] During the year 2016-17, India signed 17 bilateral agreements and MOU`s to upgrade its cyber security infrastructure at national, regional and international level

[4] B.G. Prakash, Squadron Leader (Retired). “Unborn Silicon of India”. Indian Defence Review January-March 2000, V.15(1), P.96.

[5] Export value of IT software and services from India from FY 2009 to FY 2018, 26 October 19, https://www.statista.com/statistics/320753/indian-it-software-and-services-exports/

[6] Lieutenant Colonel Mir Waqar Hussain.”IW-Options for Pakistan”, Paper, Armed Forces War Course 2001/2002, National Defence College, May 2002; Akshay Joshi, “IT-Advantage India”, IDSA, April 2000 Vol. XXIV No.1 and his article, "India's Use of IT in International relations "Indian Defence Review October-December 2000, V.15(4).

with countries like United Kingdom, United States, Israel, France, Australia, Bangladesh, Indonesia, Malaysia, Mauritius, Qatar, Portugal, Singapore and United Arab Emirates.[7]

7. Indian Defence Cyber Agency (DCA). India has recently operationalized its Cyber Command/ DCA under Tri-Services Command in Delhi. It is a highly capable, well-dispersed modern agency which would greatly enhance Indian force's cyber outreach. Its Tri-service nature means that it would include as many as 1000 personnel from all three branches, the Army, Navy and the Air force.[8] With well distributed units all across India this command has offensive and defensive cyber capability which if brought against Pakistan can be very potent. Large deployment of Indian Armed forces on our eastern border with offensive cyber capability can present formidable challenges cyber and electronic warfare (EW) challenges for our military equipment and gadgetry.

8. Vulnerabilities and Likely Targets.[9] Indian cyber threat is no more a myth. With its commercial and military cyber capability, it can effectively engage wide range of civil and military targets simultaneously. Few of the most probable targets will be:

a. Military. Most of our modern military equipment is embedded with chips and processors which renders it extremely vulnerable to cyber-attacks. Moreover, there is a large quantity of foreign equipment (specially IT equipment) held on inventory of armed forces, which increases chances

[7] The Center for Internet and Society, "Mapping of India's Cyber Security-Related Bilateral Agreements", December 2016, https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map.

[8] Nidhi Singh, " India's new Defence Cyber Agency",15 May 2019 https://www.medianama.com/2019/05/223-indias-new-defence-cyber-agency-nidhi-singh-ccg-nlud/

[9] Alan D. Campen, Douglas H. Dearth and R. Thomas Goodden, eds. Cyberwar: Security, Strategy and Conflict in information Age. (New Delhi: Bookmart Publishers, 2000), P.192.

of cyber espionage and attacks. Few of the main targets would remain to be:

(1) Command, Control, Communication and Intelligence Systems.

(2) Surveillance and Early Warning Systems.

(3) Electronic Warfare Systems.

(4) Target Acquisition Systems.

(5) Missile Guidance and Fire Control Systems.

(6) Identification of Friend and Foe (IFF) Systems.

(7) Satellite data for GPS.

(8) Strategic communication systems.

b. Civil. Like military targets, civil computer networks and communication systems are equally vulnerable to the cyber-attacks. These assets are equally important and any damage to them can greatly affect our national war fighting capability. Likely targets are:

(1) Fixed telecommunication and cellular networks.

(2) Government records, websites and databases.

(3) Private Enterprises.

(4) Power hubs and national grid stations.

(5) Air traffic control systems.

(6) Banking and financial systems.

(7) Electronic and social media.

(8) Transportation systems.

9. Threat Manifestation. Our adversaries while using its IT potential would use all means to create a cyber dilemma for us. Website defacement, spear phishing and malware are most commonly used tools are most effective in conducting cyber-espionage campaigns.[10] Pakistan has been declared as the top target of cyber espionage and malware attacks globally by the Microsoft.[11] Although extremely difficult to be quantified, keeping in view the potential of our neighbour, future cyber threat can unfold in following scenarios: -

a. Unauthorised access of computer systems to obtain or alter sensitive information.

b. Injection of computer viruses into computer networks, exchanges, weapon systems and other computer-based systems.

c. Hacker activities to explore vulnerabilities of our systems in peace time.

d. Jamming of military communications through satellites/airborne jammers.

e. Using Electromagnetic Pulse (EMP) through non-nuclear means to disrupt communication and other electronic systems.

f. Placing logic bombs in digital equipment to be activated at pre-determined times.

g. Sending ominous E-mail message to those who have Internet access.

h. Mass propaganda, narrative building through website defacement and use of social media platforms.

---

[10] Center for Security Studies (CSS), "Hotspot Analysis, Regional rivalry between India Pakistan: tit-for-tat in cyberspace", August 18. ETH Zürich

[11] "Microsoft Security Intelligence Report (Volume 21)" December 14, 2016, https://www.microsoft.com/en-sa/security/Intelligence-report; Inamullah Khattak, "Pakistan top target for foreign espionage, Senate committee told," Dawn, January 19, 2017, https://www.dawn.com/news/1309413/pakistan-top-target-for-foreign-espionage-senate-committee-told.

Response Framework

10. In order to mitigate such wide-spectrum cyber threat, a strategic framework is required to be formulated. Our conventional military capability needs to be safeguarded against this invisible threat. Pakistan's Chief of Army Staff (COAS) General Qamar Javed Bajwa while addressing passing out parade of 110th Midshipmen held on 22 Dec 2018 said "You have to prepare yourself to read the environment, gauge enemy's latest moves and be ready to respond, even when a surgical strike exists only in cognitive domain or even when the attack comes, not in the battlefield but in cyber space".[12] A coherent and all-encompassing response is therefore required at the national level by carefully integrating military and civil institutions.[13] However, unfortunately large gaps exist in our present cyber capability at various levels and dimensions which merits due attention. With this perspective, following response measures are available for consideration:

a. Transformation in Mindset. There is a need to bring a change in conventional mindset by bringing more focus on dynamic IT trends. Cyber aspects should be considered important for war fighting. There is a lack of awareness about IT which should be tackled from the gross root level. IT and cyber aspects should be incorporated from the school and college level as a long-term measure. The government and military departments need to upgrade their standard operating procedures in consonance with

[12] Inter Services Public Relations, " PR-397", 22 Dec 2018.

[13] Syed Ali Hadi, "Securitization of Cyberspace: The Debatable Contours of Cyber Warfare", Hilal, 1 February 2018.

latest IT trends and inculcate more cyber awareness among the people who operate computers and other digital devices.

b. Cyber Policy Cell. This figures out to be a major requirement as presently no core body exists which can give strategic direction or guidance about cyber aspects. A policy cell comprising members of leading software firms, civil and military members may be established under ministry of science and technology. The cell should be mandated for:

(1) Make in-depth analysis of cyber threat and its manifestations across various segments and dimensions.

(2) Ascertain the country's IT potential and plans for harnessing it.[14]

(3) Formulate cyber warfare policy and capability development plans /roadmap to be implemented.

c. Setting Objectives of Cyber Warfare. Clear objectives of cyber warfare are required to be formulated in line with national cyber policy.

(1) Short Term Objectives (5 Years)

(a) Acquire self-sufficiency in operating and maintenance of computerized systems.

(b) Capability of indigenous development of software.

(c) Comprehensive screening of all equipment on induction especially military hardware.

(d) Standardization of IT and communication equipment for all government institutions.

[14] Bina Shah, "Pakistan, the Next Software Hub?", New York Times, 10 August 2015

(2) Long-term Objectives (10-15 Years)

(a) Safeguarding vital communication nodes, IT hubs and data bases against physical and electro-magnetic pulse (EMP).

(b) Develop industrial base for indigenous manufacturing of computer hardware, chips and microprocessors etc.

(c) Acquiring a credible cyber capability which act as a deterrent and a force multiplier to conventional military prowess.

d. National Policy Guidelines on Cyber Warfare

(1) Military Strategy. Cyber policy and its practical manifestation should be carefully integrated within overall military strategy. This would be coordinated through joint services headquarters on the top to allow uniform implementation of policy across three services.

(2) Education Policy. Computer sciences and IT be introduced as a special subject in the school in order to bring progressive awareness. Universities and colleges should introduce it part of main courses with an aim to produce expertise for future cyber warfare programs.[15]

(3) Cyber Warfare Policy. A team of experts from military, government, media and IT be formed which would formulate a cost effective and futuristic cyber policy.

[15] Yusuf Hussain, "Why Cyber Security is critical to our future", Hilal, 14 December, 2018, https://www.hilal.gov.pk/eng-article/why-cybersecurity-is-critical-to-our-future/MjMwMw==.html

e. Development of Cyber Warfare Capability

(1) Intelligence Setups. Conventional intelligence procedures, organizations and expertise need a paradigm shift. Special branches within these setups be introduced to mitigate and eal with specific threats in cyber domain.

(2) Information Security. Old standard operating procedures, computer systems and protocols need a substantial uplift. More focus will have to be given on the encryption and software technology. Regular checks be ensured against any breaches, violations and necessary gaps be removed.

(3) Human Factor in Cyberspace. Human factor in cyber security is one of the weakest link that is applicable even to computer users with enough knowledge and requisite training as it is more of a behavioural rather than a knowledge issue. Humans are often unknowingly and unwillingly causing cyber security breaches due to lack of awareness and careless attitude. Consequently, there is a need to continuously make people aware of cyber security and cultivate culture of positive security behaviour.[16] The most sophisticated and finest cyber security technology remains ineffective and will eventually be unsuccessful if computer users are not aware or concerned about cyber security.

[16] Brigadier, Dr Abdul Rauf, "The Importance of Human Factor in Cyber security", Hilal, 15 April 19.

(4) Contractors and Vendors. Since most of the military gadgetry is being acquired from foreign countries, there is a potential security hazard. Contractors should be held accountable for any breaches in the equipment they supply. Own checks and screening also need to be optimized to reduce this threat. Maximum indigenization specially in the field of software will have to achieved at earliest.

(5) National Cyber Research Institution. In order to track the fastpaced technological advancement in field of IT, a specialized national research institution is required. This institution will render its technical advice to the policy makers/ stakeholders to formulate or alter future course of action. It will also contribute towards developing indigenous software and hardware capability specially for military weaponry and equipment.

(6) Offensive Cyber Capability. This capability must also be given due consideration. A potent offensive cyber capability to counter enemy's attacks is need of time which would also prove to be a great deterrent. Hackers, free lancers and computer geeks may be effectively employed to check own system integrity and wage cyber attacks against enemy.

(7) Military Training Curriculum. The professional military training regime has to bring upon many changes in its curriculum so as to instil better understanding of threats, vulnerabilities and challenges

attached with cyber domain. A culture of digital security is to be nurtured in the forces amongst all ranks to curb the mal-practices and complacency in this regard.

(8) Internet as a Warfare Tool. Internet is in everyone's reach. Rather than misusing it, an effective application can bring rich dividends. A comprehensive policy be developed on use of internet keeping in view national objectives and likely threats. Maximum use of public awareness forums and focused campaigns be made in order to reduce the risks of cyberattacks.

CONCLUSION

11. Revolution in computer technology has brought significant changes in conventional warfare. Indo-Pak scenario being no exception, is equally influenced and is likely to remain so in future. Both countries are at parity in conventional war fighting capability, under the nuclear umbrella. Any large-scale military conflict therefore is not very probable in foreseeable future, rather more indirect/ hybrid means of war would be employed. India does have a considerable edge in IT field which if harnessed against Pakistan in cyber domain can be very effective. To deter this threat, an all-encompassing, integrated national initiatives including civil and military capabilities will have to be brought in action under a strategic vision. The response to this challenge does not lie in military domain alone. More pragmatic and phased approach with well-defined objectives will have to be enforced against this looming threat.

RECOMMENDATIONS

12. In view of the arguments/ discussion above, following recommendations are proffered:

a. Formulation of Cyber Policy cell at national level under ministry of science and technology to give strategic direction and guidance to all institutions on cyber aspects. Inter-ministerial coordination to be ensured in order to bridge the gaps and existing loopholes as so to achieve multi-level, multi-layered response.

b. Inclusion of Cyber component in conventional military strategic and operational planning processes under overall coordination of Joint Service Headquarters.

c. Introducing cyber warfare as a compulsory subject in basic military training in order to increase awareness amongst forces and change the mindset/ approach towards cyber threats and vulnerabilities.

BIBLIOGRAPHY

Ali Hadi, Syed "Securitization of Cyberspace: The Debatable Contours of Cyber Warfare", Hilal, 1 February 2018.

Campen Alan, Dearth Douglas and Goodden Thomas, eds. Cyberwar: Security, Strategy and Conflict in information Age. (New Delhi: Bookmart Publishers, 2000), P.192.

Cohen, Stephen P, "South Asia Needs a Peace Process", Asian Wall Street Journal, June 12, 1999.

Cohen, Stephen P, "Nuclear Weapons and Nuclear War in South Asia: An Unknowable Future", A Paper Presented to the United Nations University Conference on South Asia, Tokyo, Japan, May 2002.

Husain, Mir Waqar, Lieutenant Colonel. “Information Warfare-Options for Pakistan”, Paper, Armed Forces War Course 2001/2002, National Defence College, May 2002.

Inter Services Public Relations, " PR-397", 22 Dec 2018.

Microsoft Security Intelligence Report (Volume 21), 14 December, 2016, https://www.microsoft.com/en-sa/security/Intelligence-report.

Prakash, B.G, Squadron Leader (Retired).” Unborn Silicon of India”. Indian Defence Review January-March 2000, V.15(1), P.96.

Hussain, Yusuf, "Why Cyber Security is critical to our future", Hilal, 14 December, 2018, https://www.hilal.gov.pk/eng-article/why-cybersecurity-is-critical-to-our-future/MjMwMw==.html.

Joshi, Akshay. “IT—Advantage India”, IDSA, April 2000 Vol. XXIV No.1 and his article, "India's Use of IT in International relations”. Indian Defence Review October-December 2000, V.15(4).

Mehmood, Ahsan Khan, " Hybrid Warfare: A Conceptual Perspective", Hilal, 1 Feb 2018.

National Task Force on IT, “Indian IT Action Plan for Software and Hardware”, http://it-taskforce.nic.in/vsit-taskforce/infplan.htm, July 30, 2002.

Rauf, Abdul, "The Importance of Human Factor in Cyber security", Hilal, 15 April 19.

Shah, Bina, “Pakistan, the Next Software Hub?”, New York Times, 10 August 2015

Singh Nidhi, " India’s new Defence Cyber Agency",15 May 2019
https://www.medianama.com/2019/05/223-indias-new-defence-cyber-agency-nidhi-singh-ccg-nlud/.