Bi-Annual Research Journal “Journal of Education & Humanities Research”
ISSN: 2415-2366 Institute of Education and Research (IER), UOB, Quetta Pakistan
Vol.5.NO 1, 2018

CYBER WARFARE THREAT TO PAKISTAN

Aurangzeb Badini
M.Phil. Research Scholar,
Department of International Relations,
University of Balochistan

Prof: Dr, Abdul Manan Bazai Chairperson,
Department of International Relations, University
of Balochistan

Abstract

The tremendous growth in the field of Computers and Information Technology has turned the word into a global village. The phenomenon has not only reduced the distances but has also resulted into diversifying the threats, increasing the vulnerabilities, rise in fraudulent and criminal activities in the cyber domain. Cheap hardware, ease of accessibility and rise in the hacking software have opened new means in the cyber warfare infringing the privacy of individuals, organizations and states alike. Not being different, Pakistan is also facing the blunt of cyber threat in all the fields. In the article, the concept of cyber warfare has been elaborated in terms of cyber-attacks on the government, corporate and private sectors around the world to highlight the future threat that would emanate for Pakistan’s computer network, infrastructure and resources. Moreover, the weaknesses in legislative and organizational framework have been highlighted.Threats posed by various organizations and countries with respect to Pakistan have also been discussed in detail. It is feared that nonexistence or presence of weak cyber laws, lack of an effective response mechanism and organizational structure in Pakistan may make its cyberspacee a ground for the hardliner criminals, non-state actors and international players. Timely realization of cyber threats and consequences of their uncontrolled usage have to be assessed by theGovernment of Pakistan an appropriate response mechanism has to be devised to guard *against any threats arising. Beside development at policy level, there is a need for developing a strategic, tactical, technical and organizational level to deal with the menace of cyber war.*

4. **Key words:** ICT, Cyber space, Cyber Warfare.

1.2. **Introduction:**

More than three billion users access to the internet today, compared to a mere 400 million in year 2000. With internet creating new vistas for development in various countries of the world, it also manifolds the challenges in the cyber space. As the internet provided anonymity, it also creates a disregard for national borders, which may be a revolutionary trait but it would no more remain a military challenge. While focus of the government in Pakistan is on dealing with terrorism and extremism in the context of NAP, in the same mire another threat is arising i.e. threat of cyber warfare. As per the data of ISPA Pakistan there are 25 million internet users in Pakistan (Kamran, 2013). 15 million out of these use mobile internet, whereas 1.7 million broadband services have been provided to end-users. Good thing is that Pakistan is ranked 7th in Asia, whereas Malaysia and Taiwan are on 8th and 9th respectively (Kamran, 2013). With this high a ratio of internet users in all areas of Pakistan, the issue of cyberspace security is getting an important factor.

1.3. **Existing Threat - On a Cyber Plane**

Out of the many problems Pakistan is facing, Cyber security is one of the most serious one to the national security for which Pakistan is not fully prepared. We are facing a series of challenges regarding our national security in cyberspace inspite of being less advanced technologically but due to our deep dependence on internet and cyber space. These challenges are unprecedented in nature and are difficult to deal with if not impossible. As observed, there has been an enormous technological innovation in the field of ICT which has resulted into revolution in the cyber warfare domain. The impact of fifth generation warfare has also been witnessed in the cyber space. Combat soldiers have been replaced by cyber warriors, to a large extent. The battle fields of ideology, culture and religion are now being fought in the cyber domain. The revolution in ICT has also changed the concepts of intelligence and espionage with states now relying more on data and information from internet and cyber space than from human intelligence. The increased dependence upon internet and other communication means, has provided opportunities to various states to collect information through cyber snooping. It has at the same time developed the idea of e in the cyber domain from any unauthorized access. Especially the revolution in ICT in the last two decades has blessed major powers with the potential to to intercept, collect and analyze data from cybercrime and transform it into effective policy options in real time. Relevance of geography cannot be replaced, but the geo-strategist's notion “who controls this will control that” has been replaced with “who controls the information and communication domains will control the world.” As Joseph Nye and ADM William Owens, two former Harvard Professors and the Clinton Administration's Defence Department officials jointly argued almost 13 years ago, “The one country that can best lead the information revolution will be more powerful than any other.” The hegemony of the US over ICT has given them enormous power to observe, violation and recovery locked information from other smaller forces, depends on us which hardware and software. The US GWOT and the policy of targeting accuracy (also a dimension of non-kinetic warfare) to cope with the asymmetric threat by terrorists has increased the reliance upon the use of ICT. It has been made a means to combat as target identification, assessment, monitoring and supervision, and to eliminate through unmanned drones. Utilizing these technologies, US breach the privacy of small contries like Pakistan. Media exposed the news that, the most secret American Intelligence National Security Agency (NSA), garnered 13.5 billion intelligence reports of Pakistan in only one month. A huge chunk of information from the National Secrets has been recovered from the USA related to the Presidency, Prime Minister House and the national institutions in Pakistan. The main objectives were to deal with the economy, defence, security and foreign policy without any trouble. Due to the technological advancement in the country, especially its extensive use in business, the use of cybersecurity has induced vulnerability from within Pakistan as well as from abroad. This requires thorough measures to address the adverse effect of cybersecurity in Pakistan. People of Pakistan, extensively use emails, twitter, facebook and android phones for communication. These softwares and devices are constantly being monitored by the browsers from America and China, especially the facebook and emails are constantly being under surveillance by someone from distant room (Kamran, 2013).

Pakistan is vulnerable to cyber-attacks. According to Naveed Mansoor, the director of monitoring and Evaluation cell for the design and development of service from government of Sindh has mentioned that country from within and outside is continuously been facing the attacks from hackers. National bank of Pakistan has been found most affected by the hackers costing million of rupees been stolen from hackers at their ATMs. The money stolen has been found to be transferred to another account. Naveed Mansoor says "unfortunately internet security is at the top of the government."

A political party website in 2011 was found to be hijacked from a cyberattack with a message that party leaders must refrain from corruption. The website was thought shortly recovered to its original form after the incident.

The cybercrime wing in the end of 2010 arrested a hacker due to the charges of hacking the personal homepage of the president of that time Asif Ali Zaradari. From officials its was found that web page was hacked in July and was then recovered in two days. The hacker changed the name on that website by Adil "penetration" when the crime wing began to sort out the location. The accused accepted the allegation by saying he did all that just for fun. He was further delivered to the FIA for further inquiry. Similarly in the mid of 2010, the website of Punjab Police was hacked by one of an Indian hacker, leaving anti Pakistan slogans on the webpage. According to Khan (2012), Pakistan must take proper actions for the protection and security of of strategic assets and it is dangerous of not having any policy and strategy to counteract any possible attack. The armed forces and the government seem to have ignored the security threat by cybercrimes and are not found ready to face any upcoming serious threats. "Pakistan Cyber force" has emerged out to be the volunteer service in this era of economic crises in the country to defence and mitigate the serious cyber attacks.

1.4. Cyber Security In Pakistan

At national level following text highlights the present status of Cyber Attacks/ Crimes mitigation at national level:

- **Electronic Transaction Ordinance 2002.** Was passed to address the Legal aspect of electronic trading. Whereas, Prevention of Electronic

  Crime Ordinance 2009 was passed with the objective to define cyber crimes and associated fines and punishment for the criminals. The ordinance has completed its age and currently there is no cyber law in Pakistan. Electronic Crime Bill 2010 which was tabled in the National Assembly to control and combat cyber and electronic crimes is still pending approval. Nevertheless, following officers were established to enforce cyber laws.

- **National Response Centre for Cyber Crimes under FIA.** Was established to enforce the Prevention of Electronic Crime Ordinance 2009. The centre is responsible to deal with all types of electronic offences throughout the country.
- **National Telecommunications and Information Technology Security Board (NTISB)** is another government organization which deals with some aspects of cyber security in the public sector.

EXTERNAL THREATS TO PAKISTAN 1.5. **Threat from India:**

How energetically India needs to pick up an edge in digital fighting innovation is obvious from what Indian Naval Chief Admiral Sureesh Mehta disclosed to Start Post of their media cell in India. (Khan, 2011)

"The Indian Armed Forces are increasingly investing in networked operations, both singly and a joint fashion. We cannot, therefore, afford to be vulnerable to cyber-attacks. Information Technology is our country's known strength and it would be in our interest to leverage this strength in developing a formidable 'offensive' and 'defensive' cyber warfare capability. Harnessing the gene pool available in academia, private industry and the younger generation of talented individuals is imperative."

The iota of the fact is that the trends of cyber warfare is becoming more dangerous and threating than that of conventional warfare's in modern times. The trends are going in such a means in cyberspace with their varying forms like the cyber espionage, the web vandalism, disclose of calcified documents, data collection It is battled in the internet utilizing different traps, for example, the digital undercover work, web vandalism, information gathering, conveyed refusal of-administration assaults, hardware disappointment, basic foundation assaults, diminished fake material, and so on. Shah (2011)

1.6. Threat from Israel

Shah (2009) in his article writes that Israel has designed a cyber task force against the Islamic countries and more especially for Pakistan. Further he writes that a large amount of budget has been allocated for collecting information's and running espionage against them. The budget has been estimated $15000000 that is intended to carryout numerous digital instruments for collecting information's in Muslim countries. Violation of international law is very common in modern days. In the backdrop of this Israel has a huge potential to carryout digital operations against Pakistan. The main purpose of Israel is to defame Pakistan globally for propagating the misuse and demonstration of powers in the name of Islamic militants. The propaganda of Israel in Internet is very profound one in many contexts. It has created a large number of writers operating various pages against the Muslim countries and Pakistan. It has also intended to make a Hebrew website to counter the Islamic sentimental approach to pursue a large proportion of their followers. They are propagating the nuclear weapons of Pakistan are unsafe they may fall into the hands of Islamic militants. There have been prescribed innumerable Israeli websites following the propagation of defaming Islam and Pakistan. They mainly include IsrealNN.com, Israel national news.com and a German Hebrew magazine and many others orchestrating this school of thoughts. Sadia (2015) delineated that the Government of Israel has been scrutinizing the operation of Cast lead the mass killing of military in Gaza stripe in 2008. A large number of bloggers and writers have raised questions against the Israel defence minister for the mass killing of Palestinians but the Israeli government even did not feel reluctant not answer the public opinions in the social websites.

1.7. United States – Cyber Warfare Capabilities:

In the Wilson report of 2007 in the United States congress has reported that the data was always the integral part of the operations in the world. The American pressure on Pakistan is very dubious in the context of permitted link boxes. But the reasonable reply of Pakistani government is seemingly impossible to achieve. In the connection the rival countries are putting pressure on Pakistan to seek a moderate line of actions in the matter of nuclear activities. After a cyber-attack in Iran the United States of America has never alleged Pakistan of doing so. A report has been published in a leading newspaper of America the New York times that Obama administration has implemented cyber warfare against the country.

The New York Times quotes unnamed US officials, recognizing that the US "military planners have offered a much smaller computer-network attacks to prevent Pakistani distance from spots helicopters carrying Navy seal commandos in the raid that killed Osama Bin Laden on 2 May. Further he remarked that the cyber assault on the defence system of Pakistan was abandoned. The Black hawk helicopters and RQ 170 stealthy surveillance intelligence information gathering and using at in the city of Abbottabad in Pakistan. It has been reported that Osama bin laden was traced out by CIA in Pakistani compound near Abbot bad. The stealth black hawk drone 170 hovered over the city a week before conducting operation against Osama. It has been said that US may be doing such sorts of surveillance in other parts of Pakistan especially for the nuclear installations. In September 2010 Wall street journal reiterated that “many countries including the U.S., Russia, China, Israel, the U.K., Pakistan, India and North and South Korea have developed sophisticated cyber weapons that can repeatedly penetrate and have the ability to destroy computer networks".

1.8. **Panama Leaks-An Example of Cyber Warfare:**

1.9. Kundi (2014) in his article writes that the superpower countries have been using varying tools for stealing the confidential documents from the world through the help of electronic devices. They have intercepted in the affairs of their neighbour due using unfair means of cyber space. They have done all these for mere purpose of colonizing the neighbour countries they used soft powers instead of giving priority to hard powers when their way was paved out by the use of hacking system after 1945 in the world countries. Recently published data of the world by WikiLeaks and panama leaks were the tacit examples of cybercrimes launched by different countries hackers for their vested interests. In both these leakages of the panama and wiki leaks some particular countries have been targeted.

1.10. **Recommendations:**Following recommendations are proffered.

- **National Level (Kamran, 2013)**
  - ✓ The phenomenon of cyber security is a common responsibility and end users can play an important role in ensuring the security of cyber network and information systems. The masses must be made aware of

the risks they can face while staying online and must be educated about the measures they can take to prevent themselves from cyber attacks and espionage. There is a dire need hold workshops and seminars in this regard. Similarly, "National cyber security awareness day" be organized to enhance awareness amongst masses. Publishing initiatives and awareness reports, organising workshops, Public Private partnership between the experts must be ensured at national level. Keeping in view the importance of the academic institutions, mainly universities and colleges, we must start from lowest level by organising seminars, exchanging expert views, publishing and presenting researches related to this technically diversified field.

✓ Legislative frameworks be devised for cyber security. To this end, an authority at national level (that should be a joint polito-military one) be established under Prime Minister Secretariat for Cyber Security. In this connection, a bureau beestablished at the Ministry of Information Technology named "Bureau The Internet and Cyberspace affairs”.

This should act as a Command Authority tasked with modernising Pakistan cyber es, both in the military and civilian sector.It should also be a forum for developing and demonstrating offensive cyber capabilities. The objective of the cyber command must be beensure that Pakistan achieves and retains a strategic cyber deterrence. Pakistan must get the support of China in development of the Cyber Command as People Liberation Army (PLA) already has worked upon this model.

✓ One of the most important aspect of cyber security is cyber e. A cyber e policy for Pakistan is need of the hour and must be developed as soon as spossible. A mechanism must be devised for detection, response and recovery as well as to retaliate and begin cyber attacks, if required, to deter and counter cyber aggression. To fight cyber warfare a professional dedicated force shall be established. A wing of such force shall be established inside military (comprising both civil and military professionals) as well to counter advanced cyber threat from countries like Israel, India and the US.

✓ A national consensus be developed for an effective and strong legislature be formed at national level to lay foundations of cyber security in Pakistan. This legislation must cover threat emanating both at National and International level.The sections of the legislation must provide an umbrella under which the law enforcement agencies and intelligence tentacles must function. Furthermore, transparent process must be evolved, with input from both public and private sector, needs to be developed for accessing data when national security is at risk. These regulatory measureshowever must not hamper freedom of speech and rights to privacy, and must be ensured that the security measures are not being abused by agencies in the name of security.

✓ With advancement in cybercrime, cyber surveillance and cyber espionage techniques, it has become difficult for the law enforcement agencies and intelligence tentacles with their outdated tools to cope up with these.Government in Pakistan lacks capabilities and apparatus needed to effectively respond to threats emanating in cyber domain. To enhance their capabilities, a smooth coordination is required between civil and military is need of the hour. The public, military, and private sectors must join hands to develop a framework for securing critical infrastructure within the country from cyber threats. National assets including financial markets, banking sector, electric grid, nuclearpower plants and sitesshall be protected on a regular basis. War-games, artificial scenarios and exercises be conducted as a matter of routine to identify the weak spots and exercise measures in case of any eventuality.

✓ **Establishment of Cyber Institute**. Due importance be given to incorporate cyber security as a subject in educational curriculums. Moreover, cyber institutes and technology parks must be established to evolve a cyber-security society and culture. PAKCERT is a case in point. This institute should be tasked to:-

➢ Organize courses, lectures, workshops, seminars and training on the subject of cyber warfare for persons responsible to operate and maintain electronic and computer systems in government and private sector.

➢ It should acquire material on the latest trends and developments in the field of Cyber Warfare and disseminate the same to various organizations.

➢ Evaluate enemy capabilities and own vulnerabilities suggest a suitable offensive and defensive response.

REFERENCES

Niccolo Machiavelli, “Discourses on the first decade of Titus Livius”, First published by Library of Alexandria in 1531.

Sehar Kamran, Senator, “Defending Pakistan through a National Cyber Security Strategy”, Policy Seminar on Pakistan’s first ever Cyber Security Strategy, Article in Report 6 on Senate Committee of E and E production, August-September 2013, www.senate.gov.pk, (Accessed in November 2016).

UzairYounus, “The threat of cyberterrorism”, Express tribune, 21 March 2016. (Accessed March 12, 2017)

Saad Zafar, Article on LPT Certification Program, “A strategic initiative to securing cyber space”, CISA, CISM, http://www.technologytimes.pk/2012/02/06/lpt-certification-programme-a-strategic-initiative-to-securing-cyber-space/, (accessed December 08, 2016).

Farzana Shah ,“Propaganda & Warfare in Cyber World”, http://paktribune.com/articles/Propaganda-%5E-Warfare-in-Cyber-World-242277.html, (accessed September 25, 2016).

Faraan Khan, 2012, http://pakistancyberforce.blogspot.com/2012/01/traitor-governments-new-plan-to-open.html, (accessed January 21, 2017).

Michael A. Vatis, “Dartmouth College, Cyber Attacks During the War on Terrorism: A Predictive Analysis”, P.22., Hanover U.S. 22 September 2001.
Farooq, Lt Col, “Cyber Aspects of Asymmetric Warfare “, Army Green Book, p-14, July 2004.

Khurshid Khan, “Understanding Information Warfare and its relevance to Pakistan”, Institute of Strategic Studies Islamabad, http://issi.org.pk/wp-content/uploads/2014/06/1379480610_58047454.pdf, (accessed February 03, 2017).

Farzana Shah, ‘‘Cyber Warfare: Pakistan’s New Battlefield’’, South Asia Global Affairs, October 2009, http://www.saglobalaffairs.com/regional/299-cyber-warfare-pakistans-new-battlefield.html, (accessed September 08, 2016).

Jaffrey Carr, Inside Cyber Warfare: Mapping the Cyber Underworld, http://www.thecybernaut.org/2010/09/india-to-increase-its-cyberwarfare-capabilities/, (accessed February 09, 2017).

Mir Waqar Hussain, Lieutenant Colonel, "IW-Options for Pakistan", Paper, Armed Forces War Course 2001/2002, National E 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".
http://forums.bharat-rakshak.com/viewtopic.php?f=3&t=5619&start=0, (accessed February 03, 2017).

Akshay Joshi, "IT—Advantage India", IDSA, April 2000 Vol. XXIV No.1 and his article, "India's Use of IT in International relations".
Nihat, 2010, http://forums.bharat-rakshak.com/viewtopic.php?f=3&t=5619&start=0, (accessed February 03, 2017).

Farzana Shah, ''Cyber Warfare: Pakistan's New Battlefield'', South Asia Global Affairs, October 2009, http://www.saglobalaffairs.com/regional/299-cyber-warfare-pakistans-new-battlefield.html, (accessed September 08, 2016).
Sadia Rasool, "Security threat in Pakistan: Causes Challenges and Way forward'', International Scietific Online Journal, Issue 12, August 2015, Joint Publication 3-13, "Joint Doctrine for Information Operations", US, October 9 1998.

Farzana Shah ,"Propaganda & Warfare in Cyber World", http://paktribune.com/articles/Propaganda-%5E-Warfare-in-Cyber-World-242277.html, (accessed September 25, 2016).

William A. Owens, Kenneth W. Dam, Herbert S. Lin, (Ed)," Box 3.3 Information Warfare and Related capabilities, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities", Page 168, Committee on Offensive Information Warfare.

Scott W. Beidleman, Lieutenant Colonel, Strategy Research Paper, Defining and Deterring Cyber Warfare, Page 26, US Army War College class of 2009.
Abdul quayyum khan kundi, "Panama leaks:cyber warfare", April 16,2016.