Pakistan Review of Social Sciences
Vol. 3, No. 1, 2022

Cyber Threat to Pakistan National Security: National Security and Threat Perception

Author

Syed Bilal Ahmad
Dr. M. Sheharyar Khan

Abstract:

In Pakistan cyber security threat is a rising issue. It is because Pakistan does not have compatible cyber security parameters. Which is enhancing more challenges for Pakistan in world? Pakistan facing cyber security dilemma in south Asia. Pakistan does not pay her attention to securing digital network. So Pakistan's national security infrastructure is also losing its strength. So this is a rising national security threat for Pakistan, here Pakistan really need to pay attention to its cyber security and make policies and strategies to secure cyberspace.

Key words: *cyber security, cyber dilemma, cyber-crime, cyber terrorist, cyber-attack, hacking aggression.*

Introduction

Non-traditional threats gained impotence than traditional threat in the international community since 21 century. A new nontraditional rising threat to the world is cyber space. Cyber space has been introduced in British science fiction in the 1980 (Betz & Stevens, 2011). But the world cyber use in 1992, it is a thing which relate to computer and computer network like internet. That time was starting of "information age" in which the threat to stolen data or information in both software and hardware form. There is no respect of borders; no one knows who stole data. It is an invisible thing. After the three decades cyber space is introduced in military doctrine. Now cannot say that cyber space is our internet use in our home computer, global network and hardware or software. But cyberspace is a combination of telephone, television, and computer. Each and every thing is which have signals in weirs and air. So in this new world have advance or modern information and communication technology which is causes of emergence of cyber warfare. Which change the battlefield grounds from air, land, and sea toward cyberspace. According to **John Perry Barlow:** "To enter (cyberspace), one forsakes both body and place and become a thing of words alone"

After the traditional (land, sea, and air) threat to Pakistan, a new non-traditional cyberspace is a rising threat to Pakistan national security. Pakistan is facing cyber space dilemma especially in

Asia from India. Cyber space spreading in Pakistani institutions is like banking, military, government, education and digital economic sector. Pakistan does not have advance information technology, and information education. It is known Pakistan last some years paying more intention to terrorism rather than advancement in information technology. So cyber war is a big dangerous threat to Pakistan national security which threat is also called 5th generation war. Pakistan still affected by some little cyber space attack, increasing cybercrime, lack to securitize his information. Pakistan has good policies, laws, decision making and bills on cyber space crime but unfortunately, there is no proper implementation on these laws and policies. Pakistan should have to effective work on this particular area.

Significance of this study

"Cyber threat to Pakistan national security" reason of this topic chosen is that Pakistani administration and people do not aware from the threat of cyber space war and tensions to national security. This paper will help to understand the terms like cyber space, cyber warfare, and cyber dilemma. After the studying of this research paper Pakistani government identifies their gaps and loopholes and pay intention to this particular area and try to solve this threat, with new policies, laws and implementations.

This research paper will help to how much world is advance in information technology especially in Asia like India, Russia, and china and how they threaten the national security of Pakistan? And tell us on which things Pakistan have to pay attention. People and government are able to understand new trends and roles of international world and advancement in information technology, cyber weapons, and cyber security.

Research questions:

QUESTION NO 1:

To what extent the evolving cyber warfare strategies in world pose threats to Pakistan's national security?

Theoretical framework/Discussion

This paper studied under three main theories offensive realism, defense realism, and securitization. Offensive realism belongs to John Mearsheimer. And defensive realism belongs to Kenneth Waltz. Basically these theories state that is a country have advance and modern weapons (convention and non-convention) that can reduce the arm race and also possibility of attack of another state. But offence and defense realist argue that international politics is fundamentally conflicting. Offence and defense theories help in making of foreign policies of state. Sometime state makes offensive policies (deployment, proxy wars, and economic decline of any country) sometime state make defensive policies for their interest.

Offensive realist believes that intentionally threat to the national security of other country. Impose conflict on other for state interest, conflict is necessary of international conflict "either I kill you or you will kill me" (Shiping, 2008). Defensive realist believes that do not intentionally threat to the national security of state. But no believe that solution of everything is conflict but believes on that corporation and alliances is also way of resolving international conflict, but still make your defense system and military strong for future or conflicting situation.

In this paper use this theories offence and defense because cyber threat is newly emerging threat for Pakistan and international community. So first is defensive cyber system, mean a country should be able to defend its cyberspace system. So that their economy, civilian, personal data, information will be in strongbox. This can be done through advance and defensive information technology (IT) and cyber defense system force (mean educate, and pick those people who are good in hacking give them government jobs so they work for country stability) then Pakistan considers as defensive in cyber security domain. After gaining cyber defense system next step is cyber offence system a country should be able to use offensive cyber system and able to brock down other defensive cyber system take personal information and use this for state interest and security purposes. But Pakistan should need to work on both first defensive cyber systems then on offensive cyber system then to secure the national security because a famous quote is that "offence is the best defense"

So the third theory which is apply in this paper is securitization theory this theory developed in Copenhagen school developed the theoretical framework of the concept of securitization in the constructive domain which is centered on the collective work of **Barry Buzan and Ole Waever** (Hadi, Feburay 2 2018) The concept entails the construction of threat. Securitization act have four main component **1)** a securitizing actor: an entity that make the securitizing move. **2)** An existential threat: an object that has been identifies potentially harmful. **3)** A referent object: an object that is being threatened and needs to protected**4)** an audience: aware the target population with the security threats.

By Appling this concept of securitization fifth dimension of war (cyber warfare). Actor (Pakistan state) declare that cyberspace is a threat to national security than the actor(state) identify and pose that this treat is an existential threat (attack from cyberspace) then this threat directed toward referent object (critical infrastructure of cyber) which is to be protected. And at last target audience (nation of Pakistan) initiate activism about cyber threat and how securitize from the threat actors (civilian-military bureaucracy).

Cyber space warfare in world.

Cyberspace effect on many things like human activity, culture, economy and military. Economy or digital economic attack and threat are danger to international security. Like if some country got a military strike it will be possible to retaliate that attack equally to other county. But if a country got a cyber-attack like digital economy, country banks, personal military data, government webs hacked that county economically down so it is difficult to answer that cyber-attack equally.

As it know that computers do not think what they are doing. It is a man who do everything give command to the computer a then computer working on it. Cyber threat is not from computers and internet it is from states and its cyber force (humans) who have conflicting mind, who use this technology for crime. Now days developed states have strategies and institutions to save and secure the data and have ability to attack on another state means cyber offence.

So now it knows that future of the wars connected with the technology, guided system, command and control. First time cyber-attack use in golf war 1991. **AF/91** was a computer virus which is used by US in golf war against Iraq which damaged the air defense system of Iraq. Some agents of US smuggled this virus (hidden in a printer chip) into Iraq through Jorden. This virus disables the air defense system of Iraq.

"***Titan Rain***" in 2005 is a cyber-attack by Chines hacker against United States (Hadi, Feburay 2 2018, p. 65). In which they damaged the **lockhead Martin** (aerospace technology) in the state of Florida. This attack was an 'Advance persistent threat (APTs). This attack was state sponsored espionage attack by people liberation army (PLA).***GhostNet*** is discovered in 2009. This is also made by chines. This cyber weapon attack on political, economic, and media locations. It targeted different NGOs and diplomats. China always cyber-attack on US economic deal documents and stolen them for their own benefits and damage US economically.

Latest attacks like Estonia got cyber-attack series in 2007 from Russia. Russia targeted Estonian websites of organizations, ministries, newspaper, broadcast, parliament, and banks throughout the month. So Estonia had shut down its system and its economy was damaged and online transactions was stopped at internal and external level.

Georgia attacked by Russia in 2008, 20 July. This also kind of Estonian attack. This attack done by "zombie "computer. This attack damages the Georgian president website, TV websites etc., for 24 hours.

So most important and latest attack **Stuxnet** in 2010 culminates a whole new wave of cyber-attack over time. Stuxnet is a malicious computer worm. Stuxnet attack on the SCADA (supervisory control and data acquisition) system of Iran and damaged the nuclear program of

Iran. When Iran got nuclear weapons their president visited the place of nuclear weapons and his picture was leaked in these picture US saw SCADA box and its secret number behind the president. Through this number US inject virus in the nuclear program of Iran. This attack was a state sponsored attack. United States and Israel admitted the responsibility of worm which they jointly built.

As India is more advance in information technology so India also done cyber-attacks in Pakistan. In 2010 Pakistan to an attack name "**operation hangover** (Chandio, August 13,2015)" in this attack India targeting Pakistani government and military agencies and stolen personal information for national security interest. And after that Pakistan got second attack name "**black dragon Indian hacker squad**" in which they defaced Pakistani websites Pakistan people party (PPP), Pakistan railway, national university of modern languages (NUML), Quaid-e-Azam College Gujranwala, Pakistan Electric Power Company, and National Manpower Bureau.

Threat to Pakistan national security.

As we studied that in world countries like Russia, china, and India and US (influence in south Asia like Iran and Iraq) all these countries are more advance in cyber space technology (Nevill, 2016). So the advancement of these countries in information technology is a huge threat to Pakistan national security. Pakistan face cyber security dilemma in world. It known government of Pakistan focuses on fighting terrorism and extremism under National Action Plan (NAP). Pakistan did no pay attention to rising non-traditional threat ***"cyber warfare".*** Cybercrimes are rising rapidly in Pakistan. In Pakistan 15 million users of cell phone and 30 million users of internet. According to Federal investigation agency (FIA) cybercrime unit (CCU), 62 cases were reported in 2007, 287 cases in 2008, and 312 cases resisted in 2010. But huge number of cases is no reported.

Causes and challenges to the security of Pakistan

Causes

In Pakistani banks, banking system expanding from hardware to digital network and providing online facilities to their customers. But banks do not have advance system to encounter the illegal access to any account. So the main and common issue is hacking of ATM. Hackers install skimmer devices in ATM and stole data of ATM cards and gets money. In Pakistani bank like Allied bank, site was hacked and hackers write on the website your system is not secure.

Banks do not pay attention to the advancement of securing data technology because they said they have insurance policies. But public of Pakistan are affected by these cyber-attacks.

Pakistani government also does not pay attention to the advancement of information technology and information technology education. Japan spend 25 % budget on advance technology but Pakistan spend less than 1% on technology so there is need to pay attention on IT.

Cyber warfare is more danger and tricky than traditional threat between India and Pakistan. AsPakistan do not pay attention to technology on the other hand India pay much and more attention to the technology and very much advance than Pakistani technology. Both countries do cyber-attack on each other and hack websites both countries have cyber force. But Indian cyber force and technology is more effective than Pakistani force and technology.

In Pakistan an organization working on awareness of cyber program. Pakistan Information Security Association (PISA) takes initiative and organizes seminars and conferences. But the government pays little attentions to this awareness.

In Pakistan there is a department which hold the cybercrime matters "national response center for cyber-crime" (Rasool, August,2015)this department take action against stalling information , financial matters and terrorism but this department is not more effective because people are unaware. Also federal investigation agency (FIA) solve the problems about cybercrime related to Facebook, Google, twitter and Skype etc. but its progress is also not more effective because of lawlessness.

Challenges

Cyber security dilemma is a rising threat to Pakistan national security. Pakistan's dependency increasing on cyber space which is vulnerable for Pakistan and create some challenges.

Pakistani government banned some websites because of some objectionable data on these websites like YouTube and Torrents etc. but people got access to these sites by some other software programs like VPNs. So this is vulnerable situation for a state.

Pakistan Telecommunication Agency (PTA) is a government agency established to maintain the telecommunication. In 2012 or 2013 this agency blocked the 15380 websites/links for some objectionable data but not You Tube, so this is not much effective and alarming situation for state.

The American National Security Agency (NSA) is spying on Pakistani communication system through internet and online and hack and took the 13.5 billion pieces of E mails, phones and fax communication. After Iran Pakistan is second aim of this agency. This is alarming situation and challenge to Pakistan national security.

Banking system of Pakistan increasing their dependency on internet and online banking. But they do not have proper securitize system so there data hacked many time. Trust of people decreasing on online banking system. This is huge threat to digital economic threat to Pakistan.

Terrorist organizations have well trained people in information technology, also have advance technology. Then they done online bombing which is called cyber attacks

National Database registration authority (NADRA) is also in vulnerable situation because some Pakistani hackers said that this site is not completely secure. This site needs more protection. Because it is very sensitive site of Pakistan.

Hacktivism is increasing day by day in Pakistan. Many hackers hack and deface Pakistani government websites and government is not able to access to their own websites. It is only because Pakistan does not have advance cyber technology. This threat is from both inside and outside.

Cyber Terrorist

Cyber terrorist are very vulnerable for state and they are politically and religiously motivated and their aim is to spread fear. Problem is that they have professional skills of IT and use for cyber terrorism. They ultimately spread fear, horror and terror.

As Pakistan already faces extremism and terrorism so cyber terrorism is rising and vulnerable threat to Pakistan cyber security. They use digital network and done attacks, bombing and other terrorist activities and create threatening conditions for Pakistan.

Cyber Crimes

Here I discuss some types of cybercrime which are using in Pakistan (Rasool, August,2015)

- **Data diddling:** In data diddling hacker attack on the personal data of peoples, government and military. And use this data or information where it is needed.
- **Password hacking:** in which hacker hack the password of any website like Facebook, Gmail, and yahoo, accounts and personal websites accounts. Password hacking is very common in Pakistan which is vulnerable for people.
- **Email hacking:** in email hacking hackers easily hack the mailing accounts of the people then use these accounts for negative purpose. This is very danger for Pakistan because NASA got access to all email accounts of Pakistani people and government which is alarming situation for Pakistan but they still not take action on it.
- **Online Bank hacking:** in which also hackers attack on the accounts and password of people and hack this data files of account and passwords and use this for their own

purpose and then destroy this data. Which is very harmful for banks and stop the working of bank and cause to stop the economy of any country?

- **Salami attacks:** those attacks which completely damage any system. In this attack hackers use different types of worms and viruses which are heavier than computer or any system and use to destroy the computer.
- **Cyber stalking:** in cyber stalking, hacker continuously sends emails to a targeted person, and follow him what he doing through internet.
- **Financial crime:** in which hacker hack the targeted person credit cards, account, and money laundering and stop each and every thing and hackers use it for shopping**.**
- **Web jacking:** in which hackers hack the personal sites and owner of site don't get access to the site. This is very common in Pakistan
- **System damaging:** in system damaging hacker complete control over the personal computer PC, and laptop. Hacker hacks and destroys the personal data.

Cyber warfare against Pakistan and other Muslim countries.

Western countries already started propaganda against Muslim countries especially against Pakistan and other Muslim countries. Because Western world don't want that any Muslim country have nuclear weapons in this world. Most importantly Israel doesn't accept that, that's why they want to wagging digital network war against Islam and Muslims. According to vice news documentary **Israeli prime minister** said that *"we are spending much budget on cyber defense and offence project. And we are number one in world top five countries in cyber technology"* Israel spend **1, 50, 000, 00 $ for spying** the Pakistani strategies and data related to the information of any operation. And start propaganda against nuclear program of Pakistan through the media like BBC and FOX news also through the print media like Washington post, and New York Times. Propaganda like that Pakistani nuclear program is not under the Pakistani military it is under the terrorist and in the hand of Al Qaeda and Taliban. And spread negative information against Pakistan nuclear program. After 9/11 western countries claim that professional Taliban's in cyber space hack the websites of western countries and also claim that only Pakistan have terrorist organizations. So Pakistan has so much vulnerability from cyber warfare. Pakistan has work on it because as it knows that after attack Pakistan doesn't claim this country attack on Pakistan because this is an invisible attack. So we have to make our defense system song. And make our defensive system offensive.

Strategies for cybercrime prevention.

Cybercrime is not much different from traditional crimes. Both work for same thing but the only difference is that cyber criminals make lot of illegal money in less time and they work very fast. Pakistan can avoid these cybercrimes by just little bit sense and technology. People face cybercrime because they do not aware about that their system prevention of cyber-attacks. Pakistan just have to follow some strategies which is helpful and save us from cybercrime.

- **Pick the strong password and preserve it:** as all know that username, password and identification is important for any online account. So our password should be mixture of capital, small letters, and digits that type of password is difficult to hack. Because this is very easy for hackers to hack any password. So change password after short time by doing this there will be less chance to stole personal data from computer and online account. In Pakistan people chose very simple password like their names. So hacker easily hack that type of password. People do not aware by choosing of simple password they become easily victim of cyber-attack.
- **Keep the computer system updated:** keep your system update time to time. Because cyber criminals always use different type of danger software and attack on your computer. When some window based computer updated and download programs automatically here the criminals target and exploit the situation and break down system.
- **Place updated and anti-virus software:** hackers make some danger kind of virus and worms and sent it online in system which effect system. So for defense and tackling the danger situation introduced by anti-virus which prevents the virus and cyber-attack. People don’t have knowledge about this. So now day’s hackers make more advance virus with passage of time so keep your system update which protects your computer from harmful access.
- **Protect personal information:** personal information like phone numbers, home address, emails etc. if you want to protect your phone and computer than don’t response some unknown email or other. Because when you response some unknown thing cyber-criminal install some dangerous data in your computer so avoid these types of things.
- **Turn off computer system:** turn off your computer when you feel something going wrong or know that my computer is hacked rapidly do this and save your system. Because know that in this growing word people can’t take sudden action on cyber-attack so when people feel something is wrong turn off your computer.
- **Read the whole website privacy policies:** as it know that mostly Pakistani people when use any website a notification come to the screen people mostly don’t read that and ignore, refuse, and deny after that people face some serious issues because of our carelessness. So before doing everything read the whole websites privacy policies.

Cyber warfare

Cyber warfare is divided in four categories, first is Computer Network operation (CNO), second is Computer Network Attack (CAN) (P.Liff, 15 May 2012) third is Psychology Attack and fourth is Computer Network Defense (CND). So as it know some states are advance in IT, by cyber-attack these states access to illegal data of another state by using some different tools and techniques of cyber warfare. So another state identify and use defense mechanisms. But unfortunately Pakistan don’t have any strong or defense mechanism to save personal information. In cyber warfare Pakistan will face bad results because of Pakistan’s government carelessness about cyberspace.

Cyber Laws in Pakistan

In Pakistan having laws regulation is not much impressive. And people of Pakistan also not aware about laws and regulations. First bill pass in Pakistan is electronic transaction ordinance 2002 which deals with banking system. But first potential bill passin 2007 “Pakistan cyber-crime bill” it focuses on electronic crimes, Cyber terrorism, criminal access, electronic system fraud, electronic forgery, misuse of encryption etc. after that first time ever comprehensive law introduced in 2015 “ Prevention of Electronic Crime bill 2015” after that some amendments take place in this bill in 2016. So Pakistan has proper laws on cyber-crime and punishments discussed in bills but Pakistan doesn’t have proper implementation on these laws. And also not have advance technology, cyber force, and awareness.

Methodology

This research paper design is descriptive because this paper attempt to explore and explain the while providing additional information about topic. Data collection of this research paper is Qualitative because all data used in this paper is non-numerical data based on literature. Both primary and secondary sources are used in this paper. Primary sources are interviews from those people who are related to this field and secondary sources are books, articles and online search engine. Interviews are structural because everything was considered fixed time, place and ethics. Interviews hold on April, Thursday 18, 2019 from Sir Zafar khan from faculty of strategic studies National Defense University, Syed Ali Hadi from ISSRA, NDU, Sartaj khan MPhil student from strategic studies NDU also specialization in this field from Russia and Belgium.

Findings

- In world Pakistan have so many threat from cyberspace and cyber warfare from India, Russia, Israel, US and china.
- Pakistan does not have modern Information Technology. Pakistan should have to work on it.
- Politically Pakistani government ignores threats from cyber war or space war domain.
- Education institutes do not advance in IT so how Pakistan advances in technology war.
- Digital economic threats from other state through online hacking.

- There is no institutions, and proper cyber force that's why Pakistan face cyber security issue.
- Now before that less work had been done on topic of cyber threat to Pakistan national security.
- Very less literature is available on Pakistan cyberspace system because Pakistan does not have advance technology.
- No institutions are discussed anywhere which hold the cyber related problems. Pakistan should have to put lot of attention on cyberspace domain.

Conclusion.

In case of Pakistan's cyber security emerging challenges, it is needed to be make strong strategies and polices to secure the national security. As it know that in world Pakistan facing cyber security dilemma. In which some countries India and Russia also the United States want to put down the Pakistan because of her sophisticated technology. Pakistan should need to be more offensive rather than defensive and strengthen its cyber space army. Make proper policies and strategies to counter the cyber space attack. Self-help is also very important and solves the minor problems. Pakistan needs to secure her government, banking system, military sites and individual personal data from cyber thief.

Pakistan has law, passed bills, policies and punishments but in Pakistan here is no proper implementation on these laws and policies. So hacking and cyber-crime is enhancing day after day. Many times Indian cyber force due to advance technology hack Pakistani websites.

Pakistan should have to work on cyber space technology and enhance advance technology and educate their people with advance information technology. Pakistan should have to observe first world countries how they dealing with their cyber security issues. Watch how they secure their digital economic system. And make same policies like them.

Recommendations:

- Pakistan needs to join multilateral and bilateral treaties on cyber space security. Because they will help Pakistan to secure its digital system and more effective and they got advance cyber technology form other state.
- In Pakistan there are many talented people in hacking and hijacking. But they use their talent for negative purpose for cyber-crime and thieving. But if government picks those people and use them for positive purpose like for development sector, research and for secure cyber defense system.

- Here is needed to be education of information technology. So computer should be compulsory subject at school level and collage level. So out next generation will have knowledge about computer and know how to tackle cyber-crime.
- To enforce cyber laws, government has introduced legislative committees.
- Every public and private institutions and organization should also have professional teams to cope with these cyber-attacks. They also should have coordination with government institutions.
- Government should work on research and development of advance technology in the cyber domain.
- Pakistan also needs cyber force to develop first and second strike capability.

Bibliography

Betz, D. J., & Stevens, T. 2011. Cyberspace and the state: Toward a strategy for cyber-power. *Adelphi Series, 51(424)*, 9-34.

Chandio, K. 2015. Cyber security/warfare and Pakistan. *Islamabad policy research institute*.

Hadi, S. A. 2018. Securitization of Cyberspace: the debateable contours of cyber warefare. *Hilal*.

Khan, B. E. (Feburary 2018). Hybrid Warfare: A Conceptual Perspective. *Hilal*.

Lodhi, M. 2011. *Pak beyond crises state.* london: oxfored.

Nevill, L. 2016. Challenging opportunities for the Asia-Pacific's digital economy. In C. Samuel, & M. Sharma, *Securing Cyberspace:International and Asian perspectives* (pp. 221-231). New Delhi: Pentagon press.

P.Liff, A. 2012. Cyberwar: A new absolute weapon? The Profliferation of Cyber warfare and Interstate war. *Strategic studies(35)*, 401-428.

Rasool, S. 2015. Cyber Security threat in Pakistan: causes challenges and way forward. *International Scientific Online (12)*, 21-34.

Shiping, T. 2008. From offensive to defensive realism: A social evolutionary interpretation of China's security strategy. In R. S. Ross, & Z. Feng, *China's ascent power security and the future of international politics* (pp. 141-162). New York: Cornell University Press.