P-ISSN: 2790-6795	Annals of Human and Social Sciences	June 2021,Vol. 2, No. 1
O-ISSN:2790-6809	http://doi.org/10.35484/ahss.2021(2-I)03	[37-45]

Annals of Human and Social Sciences
www.ahss.org.pk

RESEARCH PAPER

Cyber Warfare as tool of Propaganda and its Challenges

[1]Zainab Murtaza* [2]Dr. Ali Shan Shah [3]Ghulam Qasim

1. Ph. D Scholar, Department of Political Science, GC University Faisalabad, Punjab, Pakistan (zainabmurtaza545@gmail.com)
2. Assistant Professor, Department of Political Science GC University Faisalabad, Punjab, Pakistan
3. PhD Scholar, Department of Political Science, GC University Faisalabad, Punjab, Pakistan

PAPER INFO	Received	Accepted	Published
	January 11, 2021	June 10, 2021	June 15, 2021

ABSTRACT

The aim of study is to examine the implications of Cyber Warfare as propaganda tool and how it impacts the national security of Pakistan. In this Modern world, every nation is facing financial difficulties and Cyber security threats. The internet has become integral part of life. After the end of Cold War, professionals started to analyze that the main subject of global security changed the conflict's nature. In cyber space, the threats are increasing like cyber frauds, stealing data, criminal activities and vulnerabilities. This new era of technology in shape of cyber weapon as propaganda tool is creating threat to national and regional security. It has become principle issue of international strategy. The cyber warfare is threat to state's integrity and security. It is threatening corporate, government and private sectors. Many countries started to invest in cyber security to protect their interest as for propagation. In the era of hybrid warfare, the cyber warfare also possess severe hazard to Pakistan's national security. The aim of studies to explore the awareness regarding cyber threats towards Pakistan and which type of measures should be taken by cyber department of Pakistan. The study on cyber warfare and its challenges is based on descriptive and analytical design by using qualitative techniques.

Keywords: Cyber Warfare, NR3C, Pakistan Cyber Army (PCA), Pakistani Advanced Persistent Threats, Propaganda

Introduction

With the passing of every decade, there is a visible up gradation in technologies and techniques of waging the war. Different scholars are now studying the art of cyber war. Cyber security is utilized for the protection of the internet and national security. It incorporates transmission systems, which are utilized for the transmission of advanced data across various associations and organizations over the web. Cyber security is important instrument which is depending on the unique national ways to secure and expand national interests. However Cyber warfare is an expanding danger to dependability and global security. These have no physical boundaries that threat to national security because they are using covert propaganda tactics. Due to unlimited race and covert propaganda tactics in cyber space, Cyber security has become a national need of state due to cyber warfare. Since Cyber space seems to control every field of life. The new race in cyber space and cyber security discovers new developments in policy making of every government. The governments are giving priority to these developments for their national interest. Now the Information and Communication Technologies (ICTs) are basic for monetary and social development in general assessment of government. These are important for advancement, social prosperity, national security and individual articulation. The entire economy and society has become progressively dependent on this computerized framework due to development of cyberspace. This is playing important role in fundamental functions of state. Pakistan is using cyber warfare capabilities to pursue the regional objectives in South Asia, especially to maintain and increase influence in the region. The rival state India always attempts to defame the Pakistan's image by misguiding and manipulating global media. A Research and Analysing wing (RAW) sponsored group caught in Karachi University by the end of March 2020, fuelling terrorist and propagation activities against Pakistan (Khan, 2020). These types of activities are increasing warfare threats which pose serious security concerns for Pakistan. However, social media, a relatively new phenomenon, has been evolving in its own right. While propaganda has existed for about a thousand years, it is only lately, with the rise of social media, that propaganda through social media has become a methodical process. In a relatively short period of time, it has been able to influence whole nations as propaganda tool. The effective manipulation of the public mind arises via the use of social technology techniques.The global world is changing from the traditional military force methods, financial quality, science and technology to security of state and human. Different cyber groups and non-state actors are working in cyber warfare to threat or damage other state's communication and information network.

In World War II atomic weapons, cruise and ballistic missiles were used to show power which changed the warfare scenario. Then in Cold War, the attention was on superpower strife and race of nuclear arms to show power between incredible forces. Propaganda during the Cold War included both methods: the propagation of doctrines and the demonization of individuals When Cold War ended, the main subject of global security changed the conflict's nature. The Internet uncovers its fast extension during the 1990s, programmers and hackers started participating in cyber tricks called as pranks while low-level crooks started investigating the potential for cybercrime (Gercke, 2012). Later it became tool of power globally and every state started to improve its technology in cyber space. The impact of cyber propaganda in shape of minor attacks is witnessed by Pakistan. Pakistan is facing violent attacks in last 5 years by rival states like hate speech and abuse of religious sentiments on Face book, Twitter and YouTube.

Since 2003, Pakistan is facing sever cyber-attacks. The most dangerous thing about cyber warfare is that it is not only used by cybercriminals but also used by cyber-terrorists. These attacks are organized to deteriorate the fighting capacity of state. However, many countries established new military institutions such as cyber commands to protect and counter attack. Hence, rival state India and Pakistan, saw the different chance to utilize the internet in cyberspace to deter her opponent with little danger of retribution. They try to counter and influence each other. In 1998, the hackers of Pakistan effectively infiltrated the Atomic Research Center of India (Dawn.com, 2011). From the late 1990s to present, Pakistani patriotic groups have introduced many successful campaigns, skills and tools related to hacktivism, they used these skills to damage or save websites especially on historical Days.

In recent years, Pakistan enhanced its cyber capacity in result of some incidents like cruelty generate by Cyber-channels, Cyber Jihad and Cybercrime. These are part of cyber-warfare which tried to weak Pakistan's national security. In 2013, Senator Mushahid Hussain said that the cyber warfare or cyber security threat may be affect the national defense and security of Pakistan. It can also affect the Pakistan's nuclear program, intelligence diplomacy, economy, civil aviation, education and industrial units. Cyber security is serious and permanent issue for stability and progress of Pakistan.

On the other side, Pakistani hackers also hack other state's websites on different times. The Pakistani hackers and Advanced Persistent Threats (APTs) (Former, 2019) uncovered in report on Transparent Tribe Operation Transparent by Cyber security firm, which included a lance phishing effort in February 2016 on embassies of India in Kazakhstan and Saudi Arabia. In March 2016, Trend Micro uncovered the story that similar hacking team of Pakistan was behind Operation called C-Major. Since 2012, Pakistani APT has been active. The APT made fake news websites and sent the connection by using email to download tainted records for propagation. However, Pakistan attacked by DDoS attack in 2008, when the services of State bank of Pakistan was stopped for 21 days. Something happened in 2018 when the customer data of twenty-two banks was hacked and uploaded on dark web (Ashraf, 2019). Indian cyber security collaborated with Israel which became more dangerous to Pakistan. The mobile phones of some senior officials of Pakistan were also hacked in 2019 through WhatsApp. The hackers used malware virus named Pegasus as they sent miss call or message and access to camera, micro phones, mails, passwords and contacts. After this incident, the government of Pakistan started working to protect sensitive data and information (Qadeer, 2020).

Literature Review

Different studies have analyzed the presence of inverse connection between cyber warfare and national security. Jason Andress, Steve Winterfeld discuss about the cyberspace battlefield, computer network exploitation, computer network attack and defense. The authors further discuss the non-state actors in computer network operations, cyberspace challenges and the future of cyber war. This book explains how to identify and defend a network against malicious attacks. Later on, Sanjeev Reli (2016) discussed that every time carries with it new systems and techniques for pursuing a war. This book is an endeavor to comprehend different subtleties of cyber warfare and its process to influence national security. In view of the cyber threat condition, the books suggest a system of cyber precept and cyber procedures just as hierarchical structure of different associations which a country needs to put resources in this policy.

Cyber-Threats to Pakistan's National Security

To give strict principles over the utilization of network, Pakistan approved the Electronic Crime Ordinance in 2007 (Usman, 2019). The National Response Center for Cybercrimes of Federal Investigation Agency of Pakistan tries to improve the ability of administration to avert and explore Cyber Crime. It is also working to secure material and give suitable information to offices and basic management related to cyber threats and restoration methods. The Center is the point for global joint effort which created in 2003; it is working for intelligence of cyber security. It seeks mainly the virus attacks, stealing data, fraud of credit card cases and economic criminalities. In Pakistan, there inactive hacker groups validated attentiveness in cyber skills.

- In present, due to covid-19 the threat to Pakistan national security increased because people quarantined due to covid-19 in their homes and started their work online (Khalil B. , 2020).They digitalize their data by using Google meet, zoom, WhatsApp for meetings and uploading their data and information on Google cloud, one drive and other different apps which becomes insecure. This may be harmful if hackers supported by the rival statesfor hacking, stealing or damaging their data and information. The infrastructure of Pakistan has been attacked by hackers many times in history e.g. banking centre, NADRA and armed forces information and infrastructure. This situation is definitely alarming for national security.

Meanwhile, Pakistani hackers are also working to secure data and deterring enemy by utilizing multiple strategies. In November 2008, for first time Pakistan Cyber Army (PCA) worked in the mutilation of the Indian Oil and Natural Gas Company (Team, 2014). However, PCA apparently worked in counter after Mumbai attacks for the last defacement of the websites of Pakistani (Research, 2019). There are different tools and techniques which are used to hack and damage important data, information, documents and programs. These are awfully dangerous for the national security of Pakistan.

Cyber-Terrorism and Cyber Propaganda

Unfettered cyber-space has filled effects of fear based upon oppression, where the terrorist associations utilize computerized data medium to spread viciousness, threat and radicalism without breaking a sweat. Pakistan has just endured a million of hurdles most recent two decades because of terrorism. Pakistani military has made huge progress by destroying the traditional terrorist assaults. Nonetheless, the danger of cyber terrorism is currently representing an increasingly intense threat because of its secret nature. The attack on Bacha Khan University in 2016, Mardan, Pakistan was planned to attack by terrorists utilizing Afghan soil and the Afghan media transmission network. Similarly, the Safoora transport assault in Karachi was accepted by Janduallahfrom Afghanistan. The name of these people are Tahir Hussain, Saad Aziz and Asad-ur-Rehman, all were college students, motivated by ISIS terrorist group. These type of incidents and attacks are threat to the Pakistan's national security. The other example was the second year student NaureenLeghari who joined the ISIS terrorist group through Facebook and later security agencies of Pakistan captured her.

Cyber Propaganda is used to spread and manipulate brutality, hostility to individual and country. This sort of publicity can put any administration under monstrous tension. The impact of cyber propaganda can be seen from worldwide occasions, for example: the supposed control of the 2016 US Presidential decisions by Russia. Cyber propaganda is used to build the psyches of the voters utilizing web-based social networking. This sort of act subverts the reasonableness of any election. By such occasions in the last few years Pakistan has likewise been endured the utilization of Social Media by various political and strict developments. The ascent of TehreekLabaik Pakistan (TLP) to advance strict violence has two times placed Pakistan in troublesome occasions both in 2017-2018. TLP utilized social media such as Facebook, tweeter, YouTube etc. to expand its motivation in which the administration was powerless to keep up law in the nation. The citizens suffered a great deal in terms of physical and mental loss because of TLP.

Cyber Harassment and Lack of Public Awareness

The other name of Cyber Harassment is cyber-bullying, which is used as cyber-domain by the individuals to harass people anywhere through social media. Mostly the people who become victims are general users of social media; they are blackmailed by enemy and used for different purposes which can be against group or state. However, the effects of cyber-bullying vary person to person, but mostly cyber bullying has a destructive impact on young people. Due to this, Young people suffer physically and mentally and they experience anxiety, depression and suicidal thought.

There is another major problem in cyber-domain which is faced by Pakistan that is the absence of awareness. As users don't have limitations that's why they know how to use the social media in secure way. The people with less knowledge about social media and technology, they easily believe in fake news that consists of cyber harassment and theft. The main reason of this is the absence of the ample computer related subjects in educational curriculum of Pakistan. Even there is no authentic book about Computer knowledge that covers the Ethics and cyber-warfare of Computer. Even today in Pakistan, there is only one University named National Defense University (NDU) that offers the course related to cyber-Security as an elective subject. This is very important on the academic level and national level to make the public aware about the use of cyber-domain security and safety. In this way they can avoid to become an easy target of cyber-bullying.

Economic Disruptions

In 21th century Economic offices are highly dependent on ICT for example, E-exchange, internet business and E-banking. Such terms have made life incredibly quick, simultaneously such changes and practices have become powerless against digital assaults. In light of the fact, economic disturbance in the cyber space is considered as the most basic because it motivates cyber-warfare to hit on the economic arrangement of the state, which can make alarming situation for state. This type of attack can harm or perhaps steal the cash. It can target the banking frameworks that are legitimately connected to the state economy, because economy is one of the most important and strong pillars of state's national security. Pakistan faced this attack on low level in 2018. However, if hackers do this with proper planning, it may leave disastrous effect on economy.

Cyber Stealing

Cyber robbery means taking the cash focusing on web based exchanging and banking organizations. Pakistan witnessed such sorts of attacks in November 2018, at that time individuals denied to transfer their money by utilizing unapproved online exchange sites. Pakistani specialists were defenseless to clarify the occurrences. Web con artists and programmers have driven numerous online payment organizations to put a prohibition on Pakistan from utilizing its administrations, for example, Google Ad Sense, PayPal, Skill etc. The abuses of Pakistani Master Cards and check cards have undermined individuals' trust. In such manner, the most recent report asserted that card information of right around 20,000 clients was taken and offered to programmers on the dim web. This sort of assaults holds the possibility to put dangerous impact on the economy of any nation.

Crypto Currencies

The secretive growth of crypto currencies over most recent couple of years has pulled in risks by significant financial specialists in view of its protected and covert nature. Digital currencies are anticipated to be utilized broadly in dread financing. For a nation like Pakistan with less productive E-installments frameworks it is hard to turn away and track these risky techniques which can be used against state. This system is straightforwardly connected to its national security. There are many enlisted digital forms of money on the planet, but only some are registered. Regardless, the crypto currency is used by unregulated monetary forms. This currency is used to avoid tax illegally. As per measurements, there are nearly 2073 digital currencies in activity. The Endorsement of crypto currency changes as of state to state. There is a flat out boycott on the utilization of crypto currency exchanging in nations, for example: Lesotho, Egypt, Bolivia, Iraq, Pakistan, Nepal, Morocco and the UAE. Pakistan anyway reported a prohibition against crypto currency and State Bank of Pakistan emphatically cautioned monetary organizations against its utilization in Pakistan. However, the absence of a compelling framework against the utilization of digital forms of money prompted 60% expansion in the estimation of Pakistan's sole cryptographic money, Pak Coin. The utilization of crypto currency in psychological warfare, tax avoidance and tax evasion is not only dangerous for the economy but also for national security in bigger framework.

Cyber Physical Attacks

These attacks are also called cyber physical impact, when the programmer/hacker arrives at this present reality from his virtual PC world outcomes in a cataclysmic result. The utilization of Stuxnet PC infection by the Americans and Israelis, which contaminated the PCs of the Iranian atomic program and caused disturbance in a large number of programmable rationale controllers (PLCs) by controlling the axes used for uranium advancement process.

These types of attacks renowned as top-level assaults by nations, for example, America considers these types of assaults like basic to robotize the Supervisory control and information obtaining (SCADA) program and Information Control Systems (ICS). These attacks are used for important programs, for example, Electrical Power lattices, Water Management and much other basic foundation.

Sabotages or threat of Damages

Sabotage or threat of damages in the area of cyber fighting is considered as the assault, where the target of hacker is the PC frameworks which control basic foundations, for example, Nuclear Power Grids, Nuclear Weapons, systems of Electric Distribution, systems of Transportation, Automated Production Systems etc. Pakistan fortunately has not confronted such sort of attacks. Because, Pakistan has established atomic program and made suitable safeguard system. Furthermore, Pakistan was less privileged in Industrial control frameworks, but made advancements later. This sort of advancement in technology is important for national security and integrity of state, for instance Iran when its atomic program was hit by the Stuxnet virus, she made her program secure from damage.

Analysis of Pakistan Cyber Space and Cyber Warfare

From most recent years of cyber-attacks in the whole world, become more dangerous. Pakistani cyber space is immature and can be damaged by somebody with a little information on the PC systems. For Instance, Pakistani specialists ordered in 2008 to ban anti-Islamic websites but face difficulties because of the absence of a powerful URL separating framework little free accessible software were utilized, which effortlessly skirted the blocking framework of Pakistan Telecommunication Authority. The government of Pakistan on various events has stopped and blocked access to numerous sites that contain disrespectful and spiteful against state. It also blocked access to blasphemous and pornographic sites, but did not get fully success due to poor blocking systems. Pakistan has weak evaluating system of The Internet Corporation for Assigned Names and Numbers (ICAN) where there is a poor framework to keep up record of web information stream.

Pakistan at present has low degree of cybercrime laws and strategies, which are supposed to combat low-level cybercrime. The essential Electronic Transactions Ordinance 2002 was drafted particularly to oversee banking issues; however, Pakistan's Cyber-Crime Bill 2007, somehow, failed to properly control the mistreatment, maltreatment of electronic encryption, electronic structure distortion and electronic fraud. The present and simply first-level response to any cybercrime in Pakistan has been held as Prevention of electronic crime bill Act 2015 which is the principle drafted law in the constitution of Pakistan to fight cybercrime. It explains the predefined regions of advanced bad behavior and orders for executing computerized infringement in Pakistan. The National Response Center for Cyber-crimes was set up in 2007 and requested to the Federal Investigation Agency (FIA) on a very basic level to fight against bad behavior and cybercrime in Pakistan. It is the fundamental unit of its sort in the country. As of late, the administration took few initiatives for awareness and to educate population, for example, through PAK-CERT, Skills for all Hunarmand Pakistan, Presidential Initiative for Artificial Intelligence and Computing (PIAIC), Kamyab Jawan and National Vocational and Technical Training. The vast majority of initiatives are helpful to establish the frameworks for a progressively vigorous digital security design (Khalil, Emerging Cyber warfare threats to Pakistan, 2020).

Conclusion and Recommendations

The emergence of technologies is becoming important factor that participate in dynamic world politics. Cyber space created a big change in world politics. In Pakistan the department of technology is not getting serious attention, on the other side, India has fixed huge budget for hi-tech technology field to exceed expectations in the cyber space to overcome different competitors in the region. All types of data and information can influence lives and national security of state. Pakistan needs solution to protect its national data and information from rival states. The government should maintain back up of all type of data. Pakistan should develop its own firewall software for security against viruses. The strategy for cyber security is most important part of national security policy. Pakistan should make special national cyber security policy for the national security of Pakistani websites and technology. Pakistan should take quick measures to identify hackers. Pakistan should recruit talented patriotic hackers and modernize her agencies who work to secure Pakistan cyber space and deal with cyber threat. Pakistan must establish its strong position in cyber space because the protection of data and information is important just like the protection of human lives for the Pakistan’s national security and integrity.

References

Ashraf, M. (2019, December 31). Cyber threats to Digital Pakistan. *The Nation*:

Baezner, M. (2019). *Hotspot Analysis: Iranian cyber-activities in the context of regional rivalries and international tensions.* Center for Strategic Studies.

Baig, R. (2019, March 26). Could Offensive Cyber Capabilities Tip India and Pakistan to War? *The Diplomat*

BBC. (2019, may 1). Kashmir attack: Tracing the path that led to Pulwama. *BBC News*

Cimpanu, C. (2016, March 19). smeshapp removed from playstore because Pakistan used it to spy Indian army. *softpedia*

Desk, N. (2014, January 30). Pakistani hackers attacked 2,118 Indian websites. *Pakistan Todays*

Dawn.com. (2011, July 28). The futility of Indo-Pak cyber wars. *Dawn*:

Fazzini, K. (2019, February 27). In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides. *CNBC*:

Former, B. (2019, November 27). India and Pakistan waging a cyberwar over Kashmir intelligence. *World*

Gercke, D. M. (2012). *Understanding cybercrime: phenomena, challenges and legal response .* information and communication technology.

Haque, J. (2010, December 4). Cyber war escalates: Pakistani hackers 'take revenge, *The Express Tribun*

Haque, J. (2010, December 1). Cyber warfare: Indian hackers take down 36 govt websites. *The Express Tribun*

James A. Lewis, K. T. (2011). Cybersecurity and Cyberwarfare. *Center for Strategic and International Studies*. https://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

Khalil, B. (2020, June 28). Covid-19: Impacts on Pakistan's Cyber Security. *South Asian Journal*. http://southasiajournal.net/covid-19-impacts-on-pakistans-cyber-security/

Khalil, B. (2020, February 14). *Emerging Cyber warfare threats to Pakistan*. Modern diplomacy: https://moderndiplomacy.eu/2020/02/14/emerging-cyber-warfare-threats-to-pakistan/

Khalil, B. (2020, April 8). *India's Hybrid / Cyber threats and its regional implications*. https://moderndiplomacy.eu/2020/04/08/indias-hybrid-cyber-threats-and-its-regional-implications/

Khan, F. (2020, April 2). JIT on local RAW network finds weapons in Karachi University raid. *The News*

Khan, M. I. (2019). Cyber-warfare: implications for the national security of Pakistan. *NDU journal*.

Qadeer, M. A. (2020, June 6). The Cyber Threat Facing Pakistan, from *The Diplomate*

Rahul. (2016, February 9). Mass Cyber Attack 2016: Pakistani Hackers deface Indian Websites. *VieEns*, https://viaens.com/blog/mass-cyber-attack-2016-pakistani-hackers-deface-indian-websites/

Relations, C. o. (2020, April 22). *Global Conflict Tracker*. Council on Foreign Relations: https://www.cfr.org/interactive/global-conflict-tracker/conflict/conflict-between-india-and-pakistan

Research, C. E. (2019, November 11). Mumbai Terror Attacks Fast Facts. *CNN*, https://edition.cnn.com/2013/09/18/world/asia/mumbai-terror-attacks/index.html

Rizwan Naseer, M. A. (2018). Cyber-Threats to Strategic Networks: Challenges for Pakistan Security. *A Research Journal of South Asian Studies, 33*, 35-48.

Salik, Z. I. (2019, September 9). Pakistan-India Cyberspace Shenanigans. *the day spring*: https://www.thedayspring.com.pk/pakistan-india-cyberspace-shenanigans/

studies, C. F. (2018). *Cyber Secur Pakistan- policy framwork.* Islamabad: Centr for Golbal & Strategic Studies.

Team, T. R. (2014, June 10). *Debugging the Pakistan Cyber Army: From Pakbugs to Bitterbugs*. Threat Research: https://threatconnect.com/blog/debugging-pca-from-pakbugs-to-bitterbugs/

Techjuice. (2017, August 14). Pakistani Ministries websites hacked by Indian Hackers. *techjuice*: https://www.techjuice.pk/pakistani-ministries-websites-hacked-by-indian-hackers/

Usman, M. (2019). Cyber Crime: Pakistani Perspective. *Internationational Islamic University Journal*.https://www.iiu.edu.pk/wpcontent/uploads/downloads/journals/ilr/volume 1/num-3/Article-2-Vol-1-No-3-140119.pdf