Global Media Journal
e-ISSN: 2070-2469
HEC Recognized
Vol.XIV
Issue 01
Spring 2021
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

Threats of Hybrid Warfare in the Age of Cyber Space and Digital Media: New Intimidations to Peace and Security in Pakistan

Dr. Malik Adnan[1]
Syed Yousaf Raza[2]
Maham Shams[3]

Abstract

The case study of Pakistan was used to analyze the employment of media technology as a tool of hybrid warfare. There is a need to define new concepts of security and intimidation in order to meet the changing requirement for security. Cyberspace is closely related to cyber security, which is used by state and non-state actors as an effective means of hybrid warfare. The current issues being faced by government officials and security departments of Pakistan in the area of hybrid warfare were the subject of the study. The hybrid war has become a topic of debate among digital media professionals, political experts, technology specialists, security authorities and policy makers. The study concludes by justifying the need to protect cyberspace from exploitation by many participants after highlighting key findings to substantiate cyber space security requirements. In the age of digital media and cyberspace, the changing aspects of hybrid warfare are unique to Pakistan. The inventive tools are needed to counter the evolving challenges in hybrid warfare and have to derive an approximate to safeguard the imminent intimidations.

Keywords: *Digital Media, Technology, Cyber Space, Hybrid Warfare, Cyber Security, Pakistan*

[1] Assistant Professor, Department of Media Studies, The Islamia University of Bahawalpur

[2] Visiting Lecturer, Department Of Media Studies, The Islamia University Of Bahawalpur

[3] Visiting Lecturer, Department of Media Studies, The Islamia University of Bahawalpur.

Global Media Journal
e-ISSN: 2070-2469
HEC Recognized
Vol.XIV
Issue 01
Spring 2021
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

Introduction

Rapid expansions in the field of media technology and cyberspace have seriously affected the warfare and security concepts. The nature of conflicts and intimidations are considerably redesigned after the Cold War. The changing dynamics of international politics, the foreign affairs and armed forces cannot ensure the states' security but economic policies and socio-cultural environment also needs to be interlinked to ensure states' subsistence. In today's world, the national security has been transmuted, which is not concerned only to old-style intimidations but to various latest technological challenges as well (Naseer, Rizwan & Amin, Musarat, 2018). There are still points of failure, despite the fact that developed countries have been able to protect their cyberspace to a reasonable level. As a nation that is unable to produce or utilise cutting-edge technology, Pakistan is at a greater disadvantage when it comes to the threat of cyber warfare.

Pakistan has a lot of issues in the field of cyber space due to the volatile situation in the country. The case study of Pakistan was used to analyze the employment of media technology as an instrument of hybrid war. The changing requirements for security are the utmost requirement of the current situation. Consequently, there is an essential to define new ideas of security, challenges and intimidations of the contemporary world. The enemies have been unable to stop Pakistan from becoming a nuclear power. Being a nuclear state; it is impossible to fight against it in any way.

Due to Pakistan strategic location and its geographical area, positive role has always been played by it at global and a regional level. It is also important for world power due to its strategic location. Moreover, being a first nuclear state in the Muslim world and relation with China are some factors that contribute to its importance. With the inception of the CPEC, it is facing threats of warfare. Intelligence agencies those are hostile to them are trying to launch different type of warfare against them. Diverse tactics of hybrid warfare are being waged by the opponents. Pakistan is trying to deal with disrupt internal chaos and against different tools of hybrid warfare which are used against the country's security.

Cyber Space and Digital Communication with Cyber Media

Cyber space is defined as a platform to provide information using electronics so that electromagnetic spectrum can be created, stored, modified, exchanged and exploit information; a most popular definition in global areana. The digital communication depends on the information communication technology as today, numerous forms of digital communication are referred as the channels and tools like e-mail, android mobile phones, video conference, WhatsApp massages, blogs, web chats, podcasts, internet video clips, mobile apps, mobile banking etc. The invention of digital media technologies has changed everything. It has brought technology and the Internet to our fingertips. This technology has made lives easier for people, distances have been covered and people are connected across continents, turning the world into a true global village. In this digital era, nearly all of us wake up and habitually reach out for our smartphones to check emails and social media updates, news, and engage ourselves in conversations (Aborisade, 2012).

Global Media Journal
e-ISSN: 2070-2469
HEC Recognized
Vol.XIV
Issue 01
Spring 2021
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

Hybrid Warfare

Since the term hybrid warfare was first coined, a variety of different explanations for its meaning have surfaced. The most recent explanation for hybrid warfare describes it as "the coordinated use of multiple instruments of power that are tailored to specific vulnerabilities across the full spectrum of societal functions in order to achieve synergistic effects" (Cullen, Patrick J. & Kjennerud, Erik R, 2017).

This definition contributes a comprehensive theme of hybrid war dealing within the cyber space to create an environment for using electronic spectrum (Bachmann, Sascha Dov, 2015).

Cyber Media Technology with Hybrid Warfare

The idea of hybrid warfare is not particularly different, it represents a combination of traditional and unconventional and chaotic wars, covering economic, diplomatic and informational including psychological, cyber and misinformation as well as political warfare outside the battleground (Bachmann, Sascha Dov, 2012).

The new model of war is actually based on the capacity to hit and achieve the targeted matters as well as proceed through non-traditional armed channels, predominantly those that are important to state and military purposes. As an approach, hybrid warfare seeks to achieve broad-based consequences using simple means, such as inhibiting enemy military tasks or averting political and moral support (Ducaru, Sorin Dumitru, 2016).

Contemporary wars are not limited to bullets now as technology is spreading everywhere and in our social life too. This allows us to perform various functions of our everyday work with a single click on the mobile with android technology to google. Such severe use of media technology also produces problems for individuals, organizations and states that can be used to their advantage by other individuals, organizations and states (Beidleman, Scott W, 2009).

There are serious problems in this area due to the fact that cyberattacks can take place anywhere in the world and have an impact on other parts of the world. There are different rules for the affected and the offenders even if a connection is made. It could have serious consequences if the attack is seen as a normal one. (Davis Jr, John R, 2015).

Development in the Cyberspace Domain of Pakistan

Pakistan has become one of the growing digital economies in the universe with the rapid development of cyberspace and digital media technology. Telecommunication and cyber media contacts are growing at a rapid pace; in Pakistan as well as boosting worldwide connectivity (Korybko, A, 2017). The primary responsibility of the CERT was to minimize any destruction, provide rapid and effective recovery, preserve evidence, and prevent similar future actions, and they were developed by the Pakistan Telecommunication Authority. There are a few obstacles that the government of Pakistan needed to overcome in order to fully execute The Prevention of Electronic Crimes Act and ensure that Computer Emergency Response Team operations were carried out to the highest possible standard. The state is confronted with a number of challenges as a result of societal problems and limited resources. The National Centre for Cyber Security was established with the purpose of expanding the country's

Global Media Journal
e-ISSN: 2070-2469
HEC Recognized
Vol.XIV
Issue 01
Spring 2021
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

capabilities. In addition, the government of Pakistan intended to build capabilities in the area of cyber security in order to create locally based specialists and solutions in the field of cyber security. However, in public sectors are yet to use old tools for their procedure, despite the fact that Pakistan is introducing technological innovations. Efforts are in progress to attain a digitalized landscape and this effort proves Pakistan's commitment in the cyberspace sector for improvement. (Hadi, S. A. 2018).

Foreign involvement through cyber space in Pakistan

Insurgencies have been found in Pakistan due to its location. The outcomes of these Insurgencies are Bomb blasts, suicide attacks, and attacks on infrastructure. The Foreign hostile forces are involved in insurgencies. By using cyberspace, the foreign forces publishing as well as broadcast false and misleading media reports about development projects that cause deleterious influence on the minds of local communities. Institutions like Anti-Pakistan forces have been meddling against such wars for long. The US and Russia India, Israel, UK, Afghanistan and Iran are all involved in a conspiracy against the country (Khattak, M. U. (2019). The propaganda against Muslim countries was started by Western countries. There are other Muslim countries along with Pakistan who are at the hit list of the western countries. Western world does not want Muslim possessing nuclear weapons. Israel does not accept that Pakistan is the only state possessing nuclear weapon, that's why they launch propaganda against Islam and Muslims. The prime minister said that they are spending a lot of money on cyber project and using cyberspace for their defense and offence projects. He further added that we are the number one country in cyber technology. Israel spend 1, 50, 000, 00 $ for spying the Pakistani strategies and data related to any operation's information. Moreover, Israel also started a campaign against Pakistan's nuclear program. For this purpose, both the print and broadcast media is being used as well.

It was always the intention of the world's powers to exploit Pakistan. The surrounding area was making a number of different measures to destabilise the nation. With the invasion of Afghanistan by the Soviet Union in 1979, many people anticipated that the Soviet Union would also attempt to seize control of Balochistan, which has a port with deep sea water. An accommodating role was performed by the Baloch insurgency in this endeavour. After seizing control of Afghan land, Russia made an effort to persuade the Baloch people to stage a rebellion against the nation. This is something that the central government of Pakistan does not support. The Soviets gave the Baloch people assurances that their area would become independent and that they would be given control over it by themselves. The Soviets were responsible for upholding the objective. They want the issue of Greater Balochistan to be raised from the territory of Afghanistan. Make an effort to divide the nation of Pakistan from the country of Afghanistan (Carson, 2018).

At the moment, fifth generation warfare is still being carried out on a significant scale in Balochistan. Anti-Pakistan forces are responsible for creating an environment of lawlessness and instability. The province is causing instability in Pakistan by working via Iran, and Afghanistan is an Indian province. The province is the location of ongoing clandestine activities that are being carried out. India is engaging in a variety of endeavors that are not congruent with the principles that guide the nation. There are

Global Media Journal
e-ISSN: 2070-2469
HEC Recognized
Vol.XIV
Issue 01
Spring 2021
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

consulates located in several places around India; Afghanistan is being exploited for terrorist activities. The region of Afghanistan has evolved into a safe haven for the terrorists who are supported by India. The taking in of Kulbushan Jadav has said unequivocally that Indian participation took place. In 2016, the publication The Dawn printed an article with the heading "Balochistan via Iran and Afghanistan." The name of the Indian government's intelligence service is simply "the intelligence agency." Both the Afghan National Directorate of Security (NDS) and the RAW are complicit in undertakings that are detrimental to the best interests of the nation.

Cyber Media Technology and Challenges for Pakistan

Pakistan is a developing state where application of cyber media is in expansion process. Like many other states, Pakistan is facing several cyber war intimidations. Due to its relatively late start and low priority towards cyber media Pakistan is ranked low in the list of technological advanced nations. Pakistan is lagging behind the modern world in terms of information technology. It is therefore difficult for Pakistan to compete in this area (Afzal, S., Iqbal, H., & Inayay, M, 2012). The military as well as private sector are trying to catch the train and take advantage of network innovations. As confidence in the network grows, security and reliability are under cyber-attacks by enemy forces, especially in the context of the Indo-Pakistani situation. Pakistan cyber security vulnerabilities constitute multi-dimensional hazard environment: a general danger from west and a specific threat from old eastern enemy India. First of all, India stands out in the cyber domain along with hybrid war tactics as the strongest threat to Pakistan's national security (Awan, Jawad & Memon, Shahzad, 2016). Pakistan's civilian and defense sectors are vulnerable to cyber-attacks in times of peace and war due to the gradual extension of information technology without much emphasis on cyber security in Pakistan (Abbasi, N. M, 2013). Thus, the protection of confidential information is a priority for officials. As social networking sites provide a platform where users can interact with their friends and share personal material. However, cyber-criminals are targeting these sites to steal a user's private material, including addresses (Mehmood, Arshad, 2019).

Cyber Threats and Policies in Pakistan

The National Telecommunications has recommended policies to protect governments, organizations and their amenities from cyber-attacks. According to the Cabinet Office, "This situation has created major worries that all regulations and standards will be executed effectively and in spirit," and that "the United States is a leading nation in the area of communications and IT, primarily electronic media." The United States utilises numerous tools via "surveillance, ground and air intelligence platforms, such as satellites, recording phone conversations, filtering emails, radio monitoring, communication leaks, sensitive information, and other complicated vulnerabilities in electronic media." The websites of Pakistan have reportedly been the target of an assault by computer hackers, as stated in a report. The numbers come from the government on the federal level and from various security forces. According to some who work in the business, the Federal Bureau of Investigation (FBI) is not able to resist these kinds of assaults very well since it lacks the competent personnel necessary to monitor or halt cyber-attacks. The National Center for Cybercrime has

Global Media Journal
Vol.XIV
Issue 01
Spring 2021
e-ISSN: 2070-2469
HEC Recognized
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

an official report; the FIA's cybercrime unit cannot track such attacks by hackers through proxy servers, such as free software TOR and censorship, which allows online anonymity. Similarly, an organization is working in Pakistan for creating awareness about cyber warfare. But this awareness is not paid much attention to by the government. There is a national response center in Pakistan for the matters of cybercrime. The department took action against stalling information. The department is not more effective due to the fact that people are unaware. The problems about cybercrime are solved by the Federal Investigation Agency but its progress is not more effective due to lawlessness.

Intimidations of Hybrid Warfare and Policies in Pakistan

Keeping this scenario in mind, cyber war is multilayered, challenging and multifaceted, particularly when used in conjunction with other means of hybrid warfare. Therefore, the problems in the field of cyber warfare are increasing. This is a worrying situation for Pakistan as it does not have proper systems and is not aware of the threat at all. The main events of cyber warfare is not only limited to targeting military, but they are directed against the various social utilities as cyber warfare is not limited to the traditional domain too.

Pakistan is an important part of the world. Foreign powers have always interfered with Pakistan's internal affairs. Pakistan has been the site of a number of violent incidents, including wars, battles, insurgencies, terrorist attacks, bomb explosions, and other acts of terrorism. Direct military confrontation has become impossible since Pakistan became a nuclear power. The enemies are targeting Pakistan. Ethnic and sectarian tendencies rise as a result of supporting insurgencies. False news is used to launch media campaigns. The internet and media are involved in warfare. Pakistan is currently facing warfare from hostile intelligence agencies. (Chandio, K. 2015).

The advancement of information technology is not paid attention to by the government of Pakistan. Information technology education is also included. Pakistan spends less than 1% of its budget on technology, which is why there is a need to focus on information technology. Japan spends 25% of its budget on advanced technology. The traditional threat between India and Pakistan is not as dangerous as cyber warfare. Pakistan pay less attention to technology than India. The technology is much better than that of Pakistan. Both countries have something to do with it. Both countries have cyber force that can be used to attack each other but cyber from India. Pakistani force and technology is not as effective as force and technology from other countries.

Challenges for Pakistan

The changing aspects of Hybrid warfare in Pakistan are unique as the state faces challenges from external as well as internal fronts. The issues and challenges are: -

Internal Challenges

Internal challenges encompass the necessary elements as terrible governance, poor literacy ratio and economic system troubles as a result Pakistan these days faces an extreme power shortage.

Exploitation, law and order situation, corruption, injustice, unemployment and discrimination are the internal challenges which are being faced by society today. The governance position is worsening due to the political confusion and the government is

Global Media Journal
e-ISSN: 2070-2469
HEC Recognized
Vol.XIV
Issue 01
Spring 2021
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

unable to focus on the elementary matters due to other interruptions. Security concerns and internal issues affect Pakistan's foreign affairs. (Khan, R. M, 2011).

External Challenges

External dynamics are also very crucial and the geostrategic location of Pakistan is the critical aspects of the external domain. Haqqani network and terror activities in Indian Kashmir have been tagged as veritable arm of Pakistan Army and Indian media exploits this narrative too (Mazhar, S, & Goraya N.S, 2019).

Internal and External Security Challenges

Pakistan is having the inside and outside security issues as terrorism and war on terror also hard-pressed Pakistan into the conflicts on its western front. Terror activities in Pakistan are mainly the base of unfortunate education system, insufficient structure, unemployment and poverty. Several terror attacks carried out in Pakistan were planned by the persons who were recruited by anti-state features, misusing their spiritual, social as well as ethical philosophies (Musarrat, et, al, 2013).

Preventive strategies for cybercrime

Cybercrime is the same thing as traditional crimes as the criminals involved in both types of crimes work for the same thing but one thing differentiate between them is that cyber criminals work very fast and they make a lot of illegal money in no time. Pakistan can use latest technology to avoid crimes. People fall a prey to these cybercrime due to lack of awareness and also lack of knowledge for the prevention of cyber-attacks. Pakistan needs to follow some strategies that are helpful. (Rasool, S. 2015).

Pick a password that is strong and keep it to yourself. Moreover, any online account needs to have identification, therefore, always try to have a mixture of letters, digits and symbols in passwords because it is difficult to hack a password with capital, small letters and digits. Whereas, people in Pakistan use a simple password; so hackers easily can hack and they become easily victim of cyber-attack (Betz, D. J., & Stevens, T. 2011).

The computer system needs to be updated because Different types of software are used by cyber criminals. Therefore, when some window based computer updated and download programs Criminals can exploit the situation and break down the system. Therefore, in order to prevent the systems used modernized and anti-virus software. Hackers insert some danger kind of virus and the system was affected by worms sending it online. For tackling with the situation; is to install strong anti-virus which can prevent the virus and cyber-attack. People don't know anything about this. The hackers are making more advanced viruses. The system update protects your computer that is harmful. Another step that can be taken to prevent from cyber-attacks is not to share personal information such as phone numbers, email address and home addresses with any one. Cybercriminals install dangerous data in your computer when you respond to an unknown event. Turn off your computer when you feel unwell. It's a good idea to read the privacy policies on the website. People don't read notifications on websites and use any website without knowledge.

The Way Forward for Pakistan in the Digital Media Age

The changing aspects of Hybrid warfare are unique as in the contemporary world, Pakistan has a number of problems from internal and external fronts in the age of digital media and cyberspace. The media technologies have the ability to effect enemy forces

Global Media Journal
Vol.XIV
Issue 01
Spring 2021
e-ISSN: 2070-2469
HEC Recognized
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

and restructuring as the experiences of various states that have even now perceived the new forms of hybrid warfare verify that domestic security must be sustained at every cost. Pakistan is the only republic which is facing the full range of Hybrid warfare and Pakistan has to adopt the instant measures to comprehend the basic dynamics of Hybrid war. After the basic understandings of these dynamics of Hybrid war, it will play a vital role in developing policies to counter it and to attain the objectives of peace. Pakistan is getting the cognizance about the advancement and evolvement of cyber-attack hazard and surety in the digital media technology, although it is a fast developing area. Pakistan needs to come up with an effective approach to protect cyber security and hybrid war. Pakistan needs to organize in order to survive in the current digital age and meet the challenges of the new media technology. To tackle with the situation new strategies and innovative apparatuses are needed to counter the evolving challenges in hybrid warfare in the cyber security and digital media domain. Though, government of Pakistan has been taken some necessary steps in this regard as prevention of electronic crimes bill 2015, national response center for cybercrime, prevention of electronic crimes act 2016.However in contemporary situation there is a way forward tocope with the cyber security, media technology and cyberspace. Pakistan has to frame a comprehensive course of action on cyber security and media technology as it is vital to implement necessary security policies as intimidations related to cyber security are continuously transforming and each new day comes up with a new experiment. Consequently, Pakistan also requires advanced cyber security preparations to counter the cyberspace intimidations to ensure the national security.

Global Media Journal
Vol.XIV
Issue 01
Spring 2021
e-ISSN: 2070-2469
HEC Recognized
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

References

Abbasi, N. M. (2013). Impact of terrorism on Pakistan. Journal of Strategic Studies, 33(2), 33-68.

Aborisade (2012).The Citizen Reporter: How technology transforms journalism business through citizen reporters in Nigeria. Lambert Academic Publishing, Deutsche, Germany.

Afzal, S., Iqbal, H., & Inayay, M. (2012). Terrorism and extremism as a non-traditional security threat post 9/11: Implications for Pakistan's security. International Journal of Business and Social Science, 3(24).

Awan, Jawad & Memon, Shahzad (2016). "Threats of Cyber Security and Challenges for Pakistan," Paper presented at the International Conference on Cyber Warfare and Security, p.426.

Bachmann, Sascha Dov (2012). "Hybrid Threats, Cyber Warfare and NATO's Comprehensive Approach for Countering 21st Century Threats–Mapping the New Frontier of Global Risk and Security Management," Amicus Curiae 88, p.14;

Bachmann, Sascha Dov (2015). "Hybrid Wars: The 21 St-Century's New Threats to Global Peace and Security," Scientia Militaria: South African Journal of Military Studies 43, no. 1, p.82.

Beidleman, Scott W. (2009). "Defining and Deterring Cyber War," Army War College Carlisle Barracks PA, pp.9-10;

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

Carson, A. (2018). Secret Wars: Covert Conflict in International Politics. 238: Princeton University Press.

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

Cullen, Patrick J. & Kjennerud, Erik R. (2017). "Understanding Hybrid Warfare," in A Multinational Capability Development Campaign project, London, p.8.

Davis Jr, John R. (2015). "Continued Evolution of Hybrid Threats" *The Three Sword Magazine* 19, (28).

Dawn . (2016, March 29). "Govt Airs Video of Indian Spy Admitting Involvement.

Ducaru, Sorin Dumitru (2016). "The Cyber Dimension of Modern Hybrid Warfare and Its Relevance for Nato," Europolity-Continuity and Change in European Governance 10, no. 1, p.10.

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.

Khan, R. M, (2011). Afghanistan and Pakistan: Conflict, Extremism and Resistance to Modernity. Karachi: Oxford University Press.

Khattak, M. U. (2019). Evolution of New Indian Military Strategy: Implications for Pakistan. Margalla Papers Issue(1)

Korybko, A. (2017). Applicability of Hybrid Warfare to Pakistan: Challenges and Possible Responses. NDU Journal, 31(1), 207-228.

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

Global Media Journal
Vol.XIV
Issue 01
Spring 2021
e-ISSN: 2070-2469
HEC Recognized
ALLAMA IQBAL OPEN UNIVERSITY, ISLAMABAD

Mazhar, S, & Goraya N.S, (2019). External Challenges to Pakistan's National Security, *Journal of the Research Society of Pakistan*, Vol. 56, No. 1.

Mehmood, Arshad (2019). "Pakistan Attracts Key It Executive to Lead New National Program," The Media line, August 12, https://themedialine.org/people/pakistan-attracts-key-it-executive-to-lead-new-national-program/.

Musarrat, R., Afzal, R., & Azhar, M. S. (2013). National security and good governance: Dynamics and challenges. Journal of Public Administration and Governance, 3(1), 117-180. doi:10.5296/jpag.v3i1.3525.

Naseer, Rizwan & Amin, Musarat (2018). "Cyber-Threats to Strategic Networks: Challenges for Pakistan's Security," *South Asian Studies*, Vol.33, No.1.

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