South Asian Studies
A Research Journal of South Asian Studies
Vol. 36, No. 2, July – December, 2021, pp. 383 – 398

Cyber Warfare as an Instrument of Hybrid Warfare: A Case Study of Pakistan

Tahir Mahmood Azad
Visiting Research Fellow, Centre for Science & Security Studies (CSSS), War Studies Department, King's College London.
Email: tahir_mahmood.azad@kcl.ac.uk
Muhammad Waqas Haider
M.A. Conflict Resolution and Peace Studies, Lancaster University, United Kingdom.
Email: m.w.haider@lancaster.ac.uk

ABSTRACT

This research paper analyses the employment of cyber warfare as a tool of hybrid warfare by focusing on the case study of Pakistan. The changing domains of war in hybrid regimes complemented by the ambiguity of cyber warfare, becomes a real destructive instrument of power. Pakistan is a developing country and the cyber space of Pakistan has numerous vulnerabilities which are exploited by our adversaries time and again. Cyber space is closely linked with hybrid warfare and it is employed by both state and non-state actors as an effective instrument of hybrid warfare. The paper begins by the challenging task of defining and briefly analysing the terms such as cyberspace, cyber warfare and hybrid warfare. The research argues how cyber warfare is being linked with hybrid warfare in contemporary times. Subsequently, it attempts to analyse the existing cyberspace of Pakistan to identify its cyber vulnerabilities and how those vulnerabilities have been exploited to undermine the national security of Pakistan through cyber warfare in a hybrid domain. Additionally, the paper highlights the major findings to underpin the requirements of guarding cyber space and concludes by underpinning the need to protect the cyber space from exploitations by multiple actors.

Key Words: **Hybrid Warfare, Cyber Warfare, Cyber Security, Pakistan, Stuxnet, PRISM, World Innovation Index, Cyber Space**

Introduction

Rapid expansions in the field of cyberspace have seriously affected the warfare and security concepts. Individuals and organisations are ever more reliant on electronic communications and utilisation of cyberspace due to rapid technological innovations and lower costs of acquisition. The domain of cyberspace is equally accessible by the states and non-state actors: the developed and developing countries, Multinational Corporations (MNCs) and National Businesses, terrorist groups and criminal networks, and Al-Qaeda and Islamic State. Multiple actors, possessing diverse agendas and ideologies, have now ease of access to cutting edge technologies in the cyber domain. Hybrid warfare involves both military and non-military means in synchronisation to undermine the adversary in various domains including but not limited to Political, economic, technology, military,

security and socio-cultural affairs. These developments generate a threat in the shape of cyber warfare which is employed innovatively as an instrument of hybrid warfare. Developed nations have been able to protect their cyberspace up to a reasonable level by employing cutting edge technologies nevertheless, vulnerabilities remain there. Developing countries like Pakistan are more prone to cyber warfare as they do not have the capacity and capability to develop and employ cutting edge technologies. Pakistan is facing numerous challenges in the domain of cyber space because this field remains neglected due to volatile situations in the country. Therefore, this research paper analyses the employment of cyber warfare as a tool of hybrid warfare by focusing on the case study of Pakistan post Mumbai attacks

Defining the Key Concepts

Land, sea and air are familiar contention turfs. Cyberspace is relatively new and it is not similar to others because it is a man-made construct. Only after realising this difference, people can appreciate what people know about warfare in other media to work out which elements apply in cyberspace. Armed conflicts between nation states are incorporating cyber warfare as an important part of military doctrines. The side that can exploit information to disperse the fog of war and crack her way through this digital haze would emerge as a victor in this evolving paradigm of warfare. Cyber warfare capabilities have made it possible to achieve politico-military objectives without committing armed forces to the battleground. The frequency, intensity, and delicacy of cyber-attacks have increased manifolds over the past decade. Not only States and non-state actors but also the individuals use myriad means for preparing and placing virtual explosives in other countries through cyberspace. Keeping in view these facts, it is important to define cyberspace and associated terminologies to better comprehend the complex concepts, though no universally accepted definitions exist for these concepts.

Cyber Space

Several definitions of cyber space have been proposed but Kuehl has worked out a comprehensive definition of the cyber space after extensive research on various definitions of cyber space. Kuehl defines cyber space as, “A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies” (Robinson, Jones & Janicke, 2015). This definition gives a brief view of cyberspace by netting all the essential elements in a coherent manner.

Cyber Warfare

The term Cyber Warfare is being used widely nowadays to highlight the exploitation of cyberspace for military purposes. Cyber warfare is more complex and it poses greater challenges and novel threats to national security in contrast to other forms of warfare (Shah, 2011). Cyber Warfare can be defined as:

> Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target (Beidleman, 2009).

This definition is comprehensive and encompasses the role of state as well as non-state actors. Beidleman has amply highlighted the requirements of force, targets and actors to make it a comprehensive definition (Beidleman, 2009). This definition also identifies the problems associated with the employment of cyber warfare because the calculation of proportionate force is not possible: a single attack can have a large impact or a series of attacks may not yield the desired results.

Hybrid Warfare

Widely varying definitions of the term 'Hybrid Warfare' has emerged since it was first coined in 2002. Recently, Cullen and Kjennerud defined Hybrid Warfare as, "the synchronised use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects" (Cullen & Kjennerud, 2017). This definition was carefully developed by a project called Multi-nation Capability Development Campaign to counter hybrid warfare. However, this definition does not specify the instruments of powers because they may vary for states and non-state actors. Additionally, the definition does not explain the types of actors in a hybrid conflict. According to a definition provided by NATO, "hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives" (Bachmann, 2012, and Mallory, 2018). This definition gives a broader essence of hybrid warfare as a combination of conventional and non-conventional strategies. However, NATO has also not specified the adversaries which can be states or non-state actors. Therefore, hybrid warfare involves both military and non-military means in synchronisation to undermine the adversary in various domains including but not limited to Political, economic, military, security and socio-cultural affairs. Hybrid warfare is also described as,

"the blurring, blending and operational fusion of different capabilities and tactics into a conflict" (Ducaru, 2016).

Cyber Warfare Linkage with Hybrid Warfare

The modern wars are now fought with bits instead of bullets, botnets instead of bombs and malware instead of militias (Geers et al, 2014). Technology is getting ubiquitous and pervasive in our daily lives. It enables us to perform diverse functions of our routine through a single touch on a mobile screen or by giving a voice command to Alexa or Google home smart devices. This intensive usage of technology also creates related vulnerabilities for individuals, organisations and states which can be exploited by other individuals, organisations and states to their advantage. There are some serious issues in this domain as cyber-attacks can be conducted from anywhere across the globe while achieving its effects in another far away part of the world. Even if the connection is established, there are different set of rules governing the affected and the perpetrator. If such an attack is treated as a conventional attack on sovereignty of a country, then it can have serious repercussions. In a recent statement, US President Donald Trump vowed to use nuclear power in response to a cyber-attack on its facilities anywhere in the world (Goud, 2018, and Sanger & Broad, 2018). On the other hand, terrorists and criminal organisations can also make low cost entries into the systems. Hence, it becomes difficult to determine whether such actors are backed by some state or otherwise. The most appropriate example is the usage of cyberspace by Islamic State (IS) and other such organisations. Islamic state operates its own organisational website and many other ventures in cyberspace. The United States, despite availability of cutting edge technologies, couldn't stop the usage of cyberspace by IS. This anonymity and ambiguousness of cyber space is a significant challenge as it does not have any identity or borders.

Bachman argues that the technology will play a fundamental role in the future conflicts where various actors will employ cyber domain to execute and control hybrid attacks (Bachmann, 2015, p.82). The argument is an established fact because cyber space has been extensively utilised by state and non-state actors during recent and on-going conflicts. The hybrid warfare actors aim to achieve surprise and to seize initiative while exploitation of cyberspace serves both purposes. Ducaru says that the cyber-attacks in relation with hybrid warfare can be called the cyber domain of hybrid warfare (Ducaru, 2016, p.7). The manifested examples of this domain include Estonia 2007, Georgia 2008 and Arab Spring. Mallory is also of the opinion that the Russian invasion of Georgia in 2008 is the first classical example of cyberspace in a hybrid conflict (Mallory, 2018, p.6). General Peter (Ex-Chairman of the Joint Chiefs of Staff) argued that a well-executed cyber-attack on a vital node of cyberspace can have a catastrophic effect which can undermine the cyber domain at multiple levels ranging from local to global (Beidleman, 2009, p.6). The Russian strategy in Ukraine is also a clear

manifestation of employment of Cyber Warfare as an instrument of hybrid warfare. Russia deliberately fused and blurred multiple instruments of power including cyber warfare and employed those instruments in a synchronised manner to achieve desired results: annexation of Crimea. Information warfare, cyber warfare, electronic warfare, and physical attacks against communication infrastructures are blended together in Russian military doctrine (Ducaru, 2016, p.17). Furthermore, Russia employs these combinations along with other instruments of hybrid warfare. These changing domains of war in hybrid regimes complemented by the ambiguity of cyber warfare, becomes a real destructive instrument of power.

Bachmann argues that the hybrid threats have less commonality with the interstate wars which were seen during the previous century (Bachmann, 2015, p.14). Bachmann's argument is based on the fact that technology has altered the way of war fighting because now the distance and terrains have less significance as drones and cyber space have shrunk these considerations to a larger extent. The use of Stuxnet by the United States to attack Iranian Nuclear facilities is a manifestation of the effectiveness and implications of cyber warfare while staying far away but getting the desired effects. Similarly, the meddling in elections of other countries through cyberspace also comes under the umbrella of the cyber domain of hybrid warfare. There is a larger debate on alleged Russian role in United States elections as well as in British elections and politics largely through social media which is a sub-domain of cyberspace. Ducaru argues that the different instruments of hybrid warfare will be employed in different combinations in different conflicts where individual elements may not be that effective at its own but could have a snowball effect in combination with other elements (Ducaru, 2016, p.11). Ducaru's argument is similar to the Chinese concept of unrestricted warfare, everyone will try to innovate the blending of different instruments of power according to their environment and capabilities (Liang & Xiangsui, 1999). Cyber warfare itself can be waged in various domains, say: a series of attacks in different societal functions of a country may create disruption, denial of services and chaos. Liang and Xiangsui argued that, "The first rule of unrestricted warfare is that there are no rules, with nothing forbidden" (Davis Jr, 2015). The prediction and early warning may also not be possible as the actors in the hybrid domain will always be innovating and employing diverse instruments of power in different prepositions without following any rules. Furthermore, the use of cyberspace by non-state actors as a tool of hybrid warfare has also classical manifestations. Cyber-attacks in France in April 2015 against TV5Monde by a group called "Cyber-Caliphate" are examples of non-state actors employing cyber-attacks as an instrument of hybrid warfare (Ducaru, 2016, p.18). This group employed synchronised attacks at various levels due to which the channel remained off-air for two days.

As conventional warfare is limited to the physical domain, cyber warfare extends beyond physical boundaries as well as time. Owing to proliferation of technologies and access to information, cyber-attacks can be conducted

economically by anyone sitting anywhere across the globe. Bachmann argues that NATO has recognised cyber warfare as one of the significant hybrid threat to global peace and security in contemporary times alongside terrorism and Weapons of Mass Destruction (Bachmann, 2015, p.14). Keeping in mind the cascading effects of cyber-attacks, Bachmann has accurately placed the cyber threats at the heart of hybrid warfare because they are more ambiguous and concealed in comparison to other instruments of hybrid warfare. Finally, drawing upon the discussion, paper argues that Cyberspace is being closely linked with hybrid warfare and it is employed by both state and non-state actors as an effective instrument of hybrid warfare.

Cyber Landscape of Pakistan

Apparently, Pakistan lags behind in cyber space technologies as India has an edge over Pakistan in the domain of information technology. According to World innovation index 2015, Pakistan was ranked 131st out of 141 countries (the lowest in South Asia) while India was 81st, Sri Lanka was 85th and Bangladesh was 129th (World Intellectual Property Organization, 2015). However, it has to be noted that Pakistan has incorporated a lot of network solutions in day-to-day life ranging from banking services to e-governance in the shape of web-based services and mobile applications over recent years. Owing to these developments, Pakistan has been ranked 105th in World innovation index 2019 while India was 52nd, Sri Lanka was 89th and Bangladesh was 116th (World Intellectual Property Organisation, 2015). Therefore by analysing the table below, it can be assumed that although Pakistan has progressed in this field, yet India and Sri Lanka are far ahead of Pakistan in the innovation domain of cyberspace.

Table: 1 Global Innovation Index Comparison

	2015		**2019**	
Country	**Score**	**Rank**	**Score**	**Rank**
India	31.74	81	36.58	52
Sri Lanka	30.79	85	28.45	89
Pakistan	23.07	131	25.36	105
Bangladesh	23.71	129	23.31	116

Source: World Intellectual Property Organisation, 2015

The institutions using computer assisted technologies are vulnerable to any determined cyber-attacks. Armed Forces have also opted for use of network enabled systems and hence are prone to intrusion / disruption by the enemy. Communications sector has seen wide expansion in recent decades. Almost, the entire population is connected through modern communication gadgets. Any attack on these systems can create mass effect in a short time. The Indian space and satellite program is a great enabler in this regard. Similarly, lack of our

general awareness related to cyber security empowers exchange of information without any safeguards. In June 1998, few freelance hackers acquired access to Bhaba Atomic Research Centre (BARC) in India (Denning, 2001). Later on, they claimed that the same can be replicated against Pakistan's classified computer systems as well. A number of agencies are working on their own to develop redundancy in this field but there is a lack of coordination in the efforts at national level. Even the security organisations work in their respective spheres and they need further collaboration for a comprehensive response. Cyber-crimes are very common in everyday life however most of its cases go unreported. Furthermore, innovative means of hacking the data and even stealing the money from bank accounts is in common practice now-a-days. Cyber-crime has risen rapidly and it has affected all segments of the society, in line with global trends. General awareness campaigns have been launched by various departments and people are getting vigilant in this regard yet, it is an area which is exploited to a greater extent.

The cyberspace management structure of Pakistan was not well established until recent. National Telecommunication and Information Security Board is the major body which advises the Prime Minister / Cabinet on the matters related to telecommunication and security of information. Electronic Transaction Ordinance 2002 (ETO) was the first of the legislations to record money transfers and provides accreditation to service providers. It enables the Government as well as service providers to document and record all transactions in electronic form. Recent actions by financial watchdog Financial Action Task Force (FATF) against Pakistan are only due to the weak legislation and loopholes in the system which can be exploited by terrorists / extremist and anti-state elements for nefarious designs. Since there had been a lack of realisation as well as awareness, therefore, our legislation had not been in pace with the rest of the world. Besides ETO, Cyber Crime Bill was introduced in 2007 which focused on electronic system fraud, electronic crimes, misuse of encryption, criminal access, cyber terrorism and electronic forgery etc. However, its implementation is a grey area owing to the lack of willingness of relevant institutions. The Prevention of Electronic Crime Bill -2015 was presented in the National Assembly in July 2015 which focussed on the Development of legalisation with new investigative power, a real time collection of data under certain circumstances, electronics evidence preservation orders, and partial disclosure of traffic data(Awan, 2017, p.429). The Prevention of Electronic Crimes Act was passed in 2016 and the salient aspects of the act include: Illegal access to information system or any critical infrastructure, unauthorised copying of any data, electronic fraud, cyber stalking, hate speech, and glorification of an offence were declared as punishable offence under this act (Khaver & Yasin, 2019, p.7)**.** Pakistan Telecommunication Authority (PTA) developed the concept of Computer Emergency Response Team (CERT) for true implementation of the act and the CERT were having the primary responsibility to control and minimise any damage, provide quick and efficient recovery, preserve evidence, and prevent similar future events (Khaver & Yasin, 2019, p.7).

However, the full implementation of The Prevention of Electronic Crimes Act and optimal operationalization of Computer Emergency Response Team (CERT) is still a daunting challenge due to social issues and resource constraints.

The establishment of the National Centre for Cyber Security (NCCS) was commenced by the Government of Pakistan in June 2018 with the aim to develop "national capabilities and capacities in Cyber Security to produce indigenous professionals and solutions in the field of Cyber Security" (Pakistan National Centre for Cyber Security). Pakistan's state institutions, organisations and individuals are encountering serious challenges in cyber space owing to exploitation of various vulnerabilities in our existing cyber milieu. The Prime Minister of Pakistan launched the Digital Pakistan Initiative in the first week of December 2019. Tania Aidrus, who was working as a senior executive in Google, has returned to Pakistan to lead the Digital Pakistan Initiative to improve public services through e-governance, to impart digital skills and to foster entrepreneurship (Mehmood, 2019). However, she later resigned from the post and this initiative could not give any benefits to Pakistan. Pakistan is introducing technological innovations, ICT based infrastructure and e-government services (Tariq et al. 2013, p.15) but most of our public sectors are still practising old means for their working, however efforts are underway to achieve a digitised landscape. This initiative shows the resolve of Pakistan to progress in the domain of cyber space to reap maximum benefits.

Cyber Vulnerabilities of Pakistan

Similar to the rest of the world, Pakistan also faces several cyber warfare threats / attacks. Pakistan has remained in the top five most spied upon countries of the world in the last decade. Due to relatively late start and low prioritisation, Pakistan is lacking behind in the field of Information Technology as compared to the contemporary world. Therefore, Pakistan finds it difficult to compete in this field (Naseer & Amin, 2018,p.38). Military and private sector are endeavouring to catch the train and benefit from the advantages of networking innovations. Due to increasing reliance on networking, security and dependability are becoming exposed to cyber-attacks by hostile forces, particularly when viewed within the context of India-Pakistan environment. Pakistan's cyber vulnerabilities constitute a multidimensional threat environment: a generic threat from the West and specific threat from our traditional Eastern rival India. Primarily, India stands out as the most potent threat for Pakistan's national security in the cyber domain coupled with hybrid warfare tactics. Due to progressive expansion of Information Technology in Pakistan without considerable focus on cyber security, both civil and defence sectors are vulnerable to Indian cyber-attacks during peace as well as war. The major vulnerabilities of Pakistan's cyber space are discussed in ensuing paragraphs.

The major cyber vulnerability of Pakistan is the National Database and Registration Authority (NADRA) which is responsible for making national identity cards and storing the information of every citizen of the country (Awan & Memon, 2016, p.426). If this system is being compromised through a cyber-attack then it could have disastrous effects. The next major vulnerability is the National Power Control Centre which is located in Islamabad. It is continuously working to computerise load dispatch facilities related to the power distribution system of WAPDA. If this system gets compromised with attacks similar to Stuxnet attacks on Iran in 2010, then it can paralyse the power system of the whole country. This vulnerability can be exploited in conjunction with other instruments of hybrid warfare to achieve a synergistic effect. Next in line is the Sui Gas Network of Pakistan which is one of its own kinds with greater reliability on interconnectivity through voice, data and video links thus making it highly dependable on cyberspace and vulnerable to cyber-attacks. The communication network is the next most important factor in the domain of cyber vulnerabilities of Pakistan. The submarine cables are the core of communication networks and are highly susceptible to cyber-attacks including physical damage to the network. There are four submarine cables which connect Pakistan to the world of the internet. All of them have their landing site at Karachi. These cables include Transworld (TW1), SeaMeWe4, IMEWE - India-Middle East-Western Europe and SeaMeWe3 - South-East Asia-Middle East - Western Europe. Any damage to these cables may significantly impact the internet connectivity of Pakistan thus virtually rendering cyberspace of Pakistan at a standstill. Similarly, International Gateway Exchanges at Karachi and Islamabad form the backbone of our connectivity with the rest of the world. A cyber-attack on these exchanges may interrupt the communications and a successful intrusion into the system may be fruitful for gaining access to a lot of information which can be exploited by any adversary. Moreover, Pakistan Railways is using a very old system of communication which is relatively immune to cyber-attacks yet the chances of cyber-attacks cannot be ruled out. The Microwave Radio System is the backbone of the railway communication system duly complemented with the line communication throughout. UHF Radio System is also used for station to station communication while VHF Radio System provides communication between train drivers and station managers. These systems are susceptible to electronic warfare which is a subset of cyber space thus a deliberative misinformation on these media can cause a disastrous incident.

Pakistan is the second most spied upon country after Iran by the United States National Security Agency (NSA) which intercepted almost 13.5 billion pieces of electronic and telecommunication from Pakistan (Rasool, 2015, p.23). This figure represents a huge vulnerability of national security of Pakistan because the spying was mostly targeted upon high ranking government and armed forces officials. The armed forces of Pakistan are also getting more into technological advancements and networking by exploiting the benefits of cyberspace like armed forces of other developed countries. The rapid adoption of modern communication and information systems are also creating more vulnerability. The reliance on

computer and related networking technologies is growing but the awareness and quality of the manpower is not being developed at a similar pace. Computers are proliferating in each arm and service for diverse applications. For example, Artillery has its own fire control system based on the latest gadgetry. Air defence command and control system of guns is fully automated. The Navy is also using such systems and the Air Force perhaps is in the lead due to its own inherent needs. However, these are mostly standalone systems and will not be affected due to cyber-attacks based on networked systems. However, the intrusion into these systems cannot be ruled out owing to innovation and cutting edge technologies. The insider threats by hybrid warfare adversaries in the cyber domain cannot be ruled out. Therefore, it is the need of the time to focus on threats from cyber warfare and to adopt futuristic cyber security policy to counteract designs of adversaries / hostile nations in this domain.

Employment of Cyber Warfare against Pakistan in Hybrid Domain

Before analysing the events where cyber warfare is employed against Pakistan as a tool of hybrid Warfare, just imagine a scenario. Let's suppose that the management and control system of Tarbela dam (biggest dam of Pakistan) comes under cyber-attack and it releases huge quantities of water. At the same time, one of the nuclear power plants is compromised through a malware like Stuxnet and it explodes due to limitations imposed by cyber malware. The underwater internet connectivity is damaged and the state banks are being heisted electronically. The national power grid is being disrupted through hacking. The air traffic control of Karachi and Islamabad airports is being attacked and closed. A massive demoralising campaign is launched on social media for spreading discomfort among the public. If all of these activities are happening simultaneously or with some synchronisation then, what will be the level of chaos in the country? This is how the manifestation of cyber warfare may look like in the realm of hybrid warfare. Keeping this scenario in mind, it can be argued that as compared to many forms of traditional threats faced by Pakistan from India, cyber warfare is complex, problematic and complicated especially once employed in conjunction with other instruments of hybrid warfare.

India has consistently invested in the field of information technology over the last couple of decades resulting in rapid advances, particularly in the fields related to software development. Since, Pakistan has been unable to accord the same priority to these aspects therefore; challenges have been on the rise in the cyber warfare domain. Furthermore, India is getting help from other technologically advanced countries including Israel, in particular. This cooperation has widened the gap to the level of asymmetry in the cyber domain. India conducted its first war game related to cyber warfare operations way back in 2010 and it was named, 'Divine Matrix'(Shah, p.58). These factors induce insecurity for people as well as the state of Pakistan. Both India and Pakistan have cyber experts / hackers

working to strengthen their own defences and weaken the other's. Cyber establishments of both countries continue to attack or hack data / systems. On a comparative basis, one can assume that Indians dominate Pakistani hackers in breaking through the boundaries of our cyber walls. This creates an alarming situation for Pakistan as it neither has proper systems in place nor have general awareness of the threat. The major incidents of cyber warfare are not limited to military targets rather these are directed against diverse societal functions as described in the definition of hybrid warfare. Cyber Warfare is not limited to conventional domain as both countries may employ cyber-attacks against critical infrastructures and strategic assets which can have catastrophic outcomes (Rasool, 2015, p.23).

In the aftermath of the Mumbai attacks, the activities in the hybrid warfare domain increased manifold with a major share of cyber-attacks against a diverse range of targets. In 2009-10, India launched a massive espionage activity against Pakistan and many other countries which remained undetected for a long time until a Norwegian firm called "Norman Securities" identified and exposed the details of "operation Hangover" in 2013 (Acohido, 2013). This attack was aimed to gather data about national security matters of Pakistan and also many other companies including Telenor which is a leading mobile services operator in Pakistan (Fagerland et al, 2013). The attacks were mainly aimed against armed forces, financial networks, engineering companies, food services, automotive industry and telecommunication operators. The report by Norman Shark covered a host of strategies adopted by Indian hackers to get critical information from many countries but Pakistan was the major target. The collection of critical information and the increase in terrorist attacks in Pakistan at the same time frame may not be a coincidence and may be a well-orchestrated model of hybrid warfare. Similarly, Pakistan was the major targeted nation by the United States spying program called PRISM which was having access to the servers of all the major companies including Google, Apple, Microsoft and Yahoo. This was again a major espionage attempt along with other 13.5 billion pieces of data being collected by NSA (Greenwald & MacAskill, 2013, p.23). These cyber-attacks highly undermined the national security of Pakistan as most of the high profile officials were targeted through these attacks. In my perspective, any hostile state having access to such sensitive data can employ hybrid strategies to keep adversaries in turmoil. Pakistan remained in turmoil from 2005 till 2015, so linkages of these cyber-attacks can be established with other hybrid incidents that happened in the same timeframe.

The hacking and defacement of websites are very common tactics employed by both India and Pakistan in response to a trigger initiated by anyone. The first round of hacking websites was witnessed in 2010 when a group called ' Indian Cyber Army' hacked a large number of Pakistani websites which was responded back by a group of Pakistani hackers who hacked and defaced Indian websites (Polatin-Reuben et al, 2013). In 2012, a group of hackers called 'Vandals' conducted cyber-attacks against Pakistan through Google domain and hacked

many websites in Pakistan (Bachmann, p.84). These attacks were aimed to collect vital information from linked websites and also to achieve the denial of services. One of the major cyber-attacks was seen on the 70th Independence day of Pakistan on 14th August, 2017 when a large number of Pakistani government websites were hacked by a group of Indian hackers (Zaidi, 2017). Indian hackers defaced the websites and displayed Indian flags along with a message: happy Independence Day to India. This incident was a major setback for Pakistan on a day of significant importance. Finally, Pakistan Telecommunication Authority (PTA) had to shut down the websites pertaining to several government departments including the Ministry of Defence, Cabinet Division, and unexpectedly even the ministry of Information Technology. This news was largely exploited by media outlets as well as by social media users to spread a sense of vulnerability and dissatisfaction among the general public. It was propagated that if the government cannot protect the state assets and online services then how are they going to protect the people and their information. This can easily be linked with hybrid warfare strategies to create disharmony among public and state institutions while the exact identification of the Indian hackers group could not be established. This incident also exposed the vulnerability of cyberspace in Pakistan even at the level of sensitive state institutions like the Ministry of defence and cabinet division.

Israel is also aiding India to launch psychological campaigns against Pakistan nuclear program through cyberspace specially via social media to propagate that Pakistan's nuclear weapons may be taken over by terrorists (Sehgal, 2018). These campaigns have created discomfort among local populace as well as international audiences. Indo-Israel nexus have been employing such tactics in a coordinated manner along with other instruments of hybrid warfare to isolate Pakistan from the international community. These intentions were also evident from Indian Prime Minister Modi's statement after the Pulwama attacks (Ahmad & Ashraf, 2019). Indian hackers also tried to hack the Air traffic control systems of Karachi and Multan airports in 2017. Although, the cyber-attacks could not be successful however if these could have been successful then it would have proven disastrous and international embarrassment for Pakistan.

Findings and Way Forward for Pakistan

Pakistan is getting a gradual awareness about the emergence and importance of Cyber threat and security. However, it is a fast growing field where various elements of government, armed forces and certain segments of society are expected to work in close coordination. Pakistan needs to organise its efforts in the right direction with right focus to accrue maximum benefits while minimising vulnerabilities. In order to meet the challenges of the new millennium and to survive, concerted efforts are required at all levels. Pakistan has to evolve a coherent response strategy to effectively safeguard against the impending threat.

The challenges in the cyber domain coupled with hybrid warfare are enormous and non-linear which cannot be adequately countered through conventional kinetic strategies. A whole range of modern strategies and innovative sets of tools are required to counter the emerging challenges in the hybrid warfare domain enabled through cyberspace. Although, few steps have been taken in right direction which include Prevention of Electronic Crimes Ordinance (PECO), Prevention of Electronic Crimes Bill 2015, Prevention of Electronic Crimes ACT 2016 and establishment of National Response Centre for Cyber Crime under the auspices of Federal Investigation Agency (FIA), yet there is a long way forward to manage this borderless domain of cyberspace. This warrants an all-inclusive and well-knitted defence mechanism of Pakistan's crucial infrastructure and its command and control mechanisms. It is vital to be conscious and equipped to implement necessary security policies and take this cyber-war to the enemy's frontiers, if required. All segmented efforts should be united under the umbrella of Cyber policy and all initiatives must be overseen and executed by the Ministry of IT and communication. Pakistan needs to formulate a comprehensive and fully integrated policy on cyber technology while keeping in view the integration of efforts in different domains.

Conclusion

There is no doubt that threats related to the Cyber domain are continuously morphing and each day comes up with a new challenge. Synchronisation and interoperability of systems at government level coupled with interface of business, economic and social institutions is a prerequisite for a comprehensive response. Like civil sectors, the military is equally vulnerable to these threats. In case of any calamity or threat, the military is usually in the lead as a relief agency. However, in case of cyber-attack, armed forces will be busy in securing their own systems and may not be readily available for support. Therefore there is a need to develop understanding of this vital subject and mushroom cognizance at mass level to generate awareness. No single organisation or institution can meet the demands of a secure system which is adequately networked as well. A comprehensive national response is the least in this domain. Pakistan essentially requires the realisation of the actual and potential threats to its critical infrastructure and needs to put all out-efforts to safeguard the security of networked infrastructures of the country. Government must identify and define the national infrastructure that remains critical to the economic and national security of Pakistan. Pakistan must also remember that owing to cyber threat, it cannot remain oblivious to the advantages of the revolution in information technology. Pakistan must gear up to make best of it while defying its ill-effects. Therefore, like any other state, Pakistan also requires effective, comprehensive and futuristic cyber arrangements to counter cyber threats to ensure economic and national security.

References

Acohido, Byron (2013). "India Likely Source of Multi-nation Cyberspying," *USA Today*, https://eu.usatoday.com/story/cybertruth/2013/05/23/%20cyberspyingindia-%20hackers-apt-attacks/2352651/.

Ahmed, Mansoor & Ashraf, Maimuna (2019). "The Pulwama-Balakot Crisis: A Strategic Assessment," VII, no. 1.

Awan Jawad Hussain et al. (2017). "Security Strategies to Overcome Cyber Measures, Factors and Barriers," *Eng. Sci. Technol. Int. Res. J* 1, no. 1, p.429.

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.

BBC (2019). "Pulwama Attack: India Will 'Completely Isolate' Pakistan," https://www.bbc.co.uk/news/world-asia-india-47249133.

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

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, no. 28.

Denning, Dorothy E. (2001). "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Networks and netwars: The future of terror, crime, and militancy*, p.239.

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.

Fagerland, Snorre & Kråkvik, Morten & Camp, Jonathan (2013). "Operation Hangover : Unveiling an Indian Cyber Attack Infrastructure," Norman Shark, https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/NS-Unveiling-an-Indian-Cyberattack-Infrastructure_FINAL_Web.pdf.

Geers, Kenneth et al. (2014). "World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks," *FireEye Inc., Milpitas, CA*, p.2.

Goud, Naveen (2019). "Trump Asks Pentagon for Nuclear Attacks in Retaliation for Cyber Attacks!," Cyber Security Insiders, https://www.cybersecurity-

insiders.com/trump-asks-pentagon-for-nuclear-attacks-in-retaliation-for-cyber-attacks/.

Greenwald, Glenn & MacAskill, Ewen (2013). "Boundless Informant: The Nsa's Secret Tool to Track Global Surveillance Data," *The Guardian*, https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

Liang, Qiao & Xiangsui, Wang (1999). *Unrestricted Warfare*, PLA Literature and Arts Publishing House Arts Beijing.

Mallory, King (2018). "New Challenges in Cross Domain Deterrence," RAND Corporation Santa Monica United States, p.11.

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

Naseer, Rizwan & Amin, Musarat (2018). "Cyber-Threats to Strategic Networks: Challenges for Pakistan's Security," *South Asian Studies (1026-678X)* 33, no. 1, p.38.

"National Centre for Cyber Security," https://www.nccs.pk/.

Polatin-Reuben, Dana et al. (2013). "A System Dynamics Model of Cyber Conflict," Paper presented at the 2013 IEEE International Conference on Systems, Man, and Cybernetics, 2013.

Rasool, Sadia (2015). "Cyber Security Threat in Pakistan: Causes, Challenges and Way Forward," *International Scientific Online Journal* 12, p. 23.

Robinson, Michael Jones, Kevin & Janicke, Helge (2015). "Cyber Warfare: Issues and Challenges," *Computers & Security* 49, p.72.

Sanger, David E. & Broad, William J. (2018). "Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms," *The New York Times*, https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html.

Sehgal, Ikram (2018). "Hybrid Warfare Challenges for Pakistan," *Daily Times*, August 18.

Shah, Farzana (2011). "Propaganda & Warfare in Cyber World," *Defence Journal* 15, no. 1-2, 2011, p.56.

Syed, Rubab, Khaver, Ahmed Awais & Yasin, Muhammad (2019). "Cyber Security: Where Does Pakistan Stand?," p.7.

Tariq, Muhammad et al. (2013). "Cyber Threats and Incident Response Capability - a Case Study of Pakistan," p.15.

World Intellectual Property Organisation (2015). "Global Innovation Index 2015: Switzerland, Uk, Sweden, Netherlands, USA Are Leaders," https://www.wipo.int/pressroom/en/articles/2015/article_0010.html.

Zaidi, Mubashir (2017). "Major Pakistani Government Sites Hacked on 70th Independence Day," The Hindu, August 14, https://www.thehindu.com/news/international/major-pakistani-government-sites-hacked-by-indian-hackers-on-70-independence-day/article19493079.ece.