P-ISSN: 2790-6795	Annals of Human and Social Sciences	Jan-March 2025,Vol. 6, No. 1
O-ISSN:2790-6809	http://doi.org/10.35484/ahss.2025(6-I)32	[372-384]

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

RESEARCH PAPER

Cyber Security: A Growing Challenge to Pakistan

[1]Nida Shabbir*, and [2]Dr. Mubeen Adnan

1. PhD Scholar (International Relations), Department of Political Science, University of the Punjab, Lahore, Punjab, Pakistan
2. Associate Professor, Department of Political Science, University of the Punjab, Lahore, Punjab, Pakistan

Corresponding Author n_shabbir87@yahoo.com

ABSTRACT

Pakistan's dependence on digital infrastructure and quick adoption of new technologies have made cybersecurity issues worse. Information security breaches, cyber assaults, identity theft, a state-run digital warfare, and spying are just a few of the many challenges the nation confronts. These dangers jeopardise the commercial, industrial, and financial sectors in addition to compromising vital government and defense data. Pakistan's weaknesses are caused by things like a lack of technological know-how, antiquated regulations, and ignorance on the part of both individuals and companies. Investigating these cybersecurity concerns, their effects on national security and financial stability, and the steps that must be taken to resolve them are the objectives of this article. Utilising a qualitative technique with a phenomenological perspective, the study uses secondary sources and an exploratory and descriptive design. In order to improve cybersecurity, it highlights the pressing need for strict laws, cutting-edge technology, and international cooperation. Addressing cybersecurity issues is essential in the current digital era for societal adaptability, economic prosperity, and national security in addition to technological advancement.

Keywords: Identity Theft, Societal Adapdability, National Security, Spying, Qualitative Techniques

Introduction

The term cyber security, also referred to as information technology security, describes the procedures and safeguards used to prevent unauthorised entry, digital assaults, damage, or stealing of devices, networks, programs, and data. The objective of cyber security is to guarantee the safety, accessibility, and integrity of data as well as defend towards possible risks and weaknesses in the world of technology. The key components of Cyber Security includes Protecting sensitive data and systems against online attacks, recognizing and maintaining an eye on questionable activity and cyber threats, implementing the necessary steps to lessen the effects of cyber-attacks, putting impacted systems and information back to normal following a cyber-attack. To protect from cyber-attacks and preserve the security of digital resources, efficient cyber security combines a number of techniques, processes, guidelines, and best practices.

This century has been labelled as an Information age, where the non-traditional threat is more important than the traditional one. The technological advancement and the revolution in communication technology and information has facilitated the emergence of Cyberwarfare. It is a serious threat to national sovereignty, and security because of its wide range of domestic, international and transnational implications. Comparing to conventional crime, it is new but the destruction it has cost is not less than conventional crime. A report by risk based survey revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018. Medical

services, retailers and public entities experienced the most breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

According to new Canalys report in the second quarter of 2023, the global cyber security market rose by 11.6% year over year to reach $19 billion. The market is expected to increase from $71 billion for 2022 to $7.89 billion for the year. (Gately, 2023) Governments across the globe have reacted to the rising threat of Cyber security by providing assistance to organizations for executing successful network protection policies e.g. In the U.S., the National Institute of Standards and Technology (NIST) has made a digital protection framework. To fight with the expansion of pernicious code and help in early detection, the framework suggests consistent, continuous checking of every electronic resource. (Gately, 2023) The threats countered by digital security are three-folded, Cybercrime, Cyber-assault, and Cyber illegal intimidation. Cybercrime incorporates single entertainers or gatherings focusing on frameworks for monetary profit or to cause interruption. Panda Security framework in 2018 separated Cyber Crime into two categories for example Crimes that target networks and devices, and Crimes that utilize various devices to participate illegal activities.

From the rise of extensive cybercrime, fears of terrorists exploiting digital infrastructure, state and corporate cyber espionage, crippling disruption by cyber activists, and even suggestions of cyberspace, turned into fifth generation warfare, the issue of cyber security has become extraordinarily important to global issue. (Sadleer, 2012) Digitalization of major sectors of Pakistan is increasing the threats of data breaches in Pakistan. The status of Pakistan in Cyber security is seventh worst country in the world, and if the appropriate measures are not taken it will remain the same. In this context, the objective of this paper is to highlight the nature of cyber threats to Pakistan's National Security. It additionally distinguishes the norms, patterns and perspectives inside the national Security culture, which are hindering in the fruitful securization of digital threats in Pakistan. It also identify and analyze the challenges that government of Pakistan is facing in prevention of cybercrime with the idea of digital Pakistan and will suggest way out. The paper centers on following research questions; what are the Cyber threats to the National Security of Pakistan? What are the Pakistan's major cyber sectors and their security dilemmas, and how Indian factor is becoming a cyber-threat to Pakistan? To answer those questions secondary sources are used which includes books, research papers, seminar papers etc.

Literature Review:

It started with the work of Mr. Memon. In his article "*Security of e-government services and challenges in Pakistan"*, in 2016 he draws attention to digital regulations, dangers, and issues related to e-government services. It also suggests digital security measures for decision-makers. His article additionally aids in the development of new security procedures and plans for Pakistani residents by lawmakers and service-oriented organizations.

In 2013 *"Cyber threats and incident response capability: A case study of Pakistan",* writers Babar Aslam and Muhammad Tariq, focuses on the broad spectrum of digital threats from common place webpage vandalism to complex and ongoing digital dangers. Additionally, it assessed current reaction capabilities, and deficiencies in governmental organisations. It is anticipated that country's inadequate reaction mechanisms, organisational structure, and cyber security regulations might make its virtual space a haven for hackers and other hostile actors and individuals. It is observed that the Pakistani government needed an adequate reaction structure in order to protect from cyber-attacks, in addition to realising the risks associated with unregulated utilisation of the internet.

Study proposes a high-level organisational framework for the creation of critical cyber security entities at various levels of government that will be in charge of safeguarding the nation's cyberspace by drafting the required laws and developing the reaction plans at various levels of administration.

Miss Ahmed in June 2022 published an article*, "Cyber Security threat and Pakistan preparedness: An analysis of National Cyber Security policy 2021"*, evaluated Pakistan's existing Cyber Security Policy to determine its efficacy and preparedness to fend off Cyber threats. She used qualitative techniques to collect the necessary data e.g. policy documents, to examine the nature of Cyber Security policy.

In an article "*The rise of Cybercrime in Pakistan: A threat to Pakistan National Security",* in 2021 writer Dr. Imran and Dr. Ghulam Murtaza examines, in the light of unconventional hazards, the extraordinary and quickly expanding risk that digital age and technological warfare pose to Pakistan's national security. In order to comprehend the present situation of cyber security in Pakistan, The outcomes of this study show that Pakistan lacks modern technological infrastructure (IT), efficient strategy execution, and sufficient advancement in IT learning, which means it is vulnerable to several cyber assaults from countries including China, Russia, India, Israel, and the United States.

In an Article *"Impact of Cyber terrorism on Pakistan's National Security",* writer Shan Ali in 2022 highlighted the fundamental problems with cyber terrorism in the contemporary day. His analysis is based on point that terrorists can use internet organise, find recruits, and connect with other terrorists both inside and outside of their borders. They will probably utilise the World Wide Web's vulnerabilities or its unsupervised services to prepare, recruit, and interact during assaults, even if they might not possess the sophisticated abilities necessary for attacking delicate, important systems.

Khathan Patel and Dhaval Chudasama in their work *"National Security threats in Cyberspace,"* in 2021 provided information about the threats which world is facing due to Cyber vulnerabilities. Their point of view is that equipment in the modern day is internet-connected; there is a significant risk of hacking. Nowadays, the entire world is connected via cyberspace. These days, there are a lot of emerging illegal actions carried out online by hackers, who perform their crimes from anywhere in the world. These days, the majority of cybercrimes are motivated by money or the desire to obtain private data. Numerous digital activities that are available nowadays aid in the battle with cybercrimes. Numerous worldwide collaborations exist among nations to combat cybercrimes, involving conferences, collaborative meetings, and various other activities. These items support the countries in building their information security teams and creating an increasingly secured online environment for their own countries.

In an article "*Cyber Space management in Pakistan"*, in 2018 writer Dr, Tughral Yasmin, addresses the gaps in policy formulation and makes recommendations for developing an appropriate plan to address the new cyber threats. She believes that to combat the negative impacts of crippling digital assaults, such as interruption of government operations, loss of company and economic efficiency, and so on, digital authorities and advisers must create efficient regulations and pass laws. Regrettably, Pakistan lags far behind other countries in terms of organising its cyberspace.

In an article," *Cyber threat in a Contemporary Era: Challenges for the security of Pakistan",* in 2022 writer Mr. Rizwan, examines the potential cyber attack's effects on Pakistan's security. His point of view was that not only do ordinary individuals utilise cyberspace systems, but important institutions like energy grids, reservoirs, and online banking are also linked to digital networks. Cyber networks are connected to military facilities such as nuclear power plants and command and control systems in a similar manner. Pakistan's dependence on digital technology has made it vulnerable to ongoing

cyber-attacks. Pakistan does not yet have a suitable system in place to address the threat posed by cyber-attacks.

In her work, *"Cyber Threats to Digital Pakistan"* in 2021 Miss Ashraf explains that the heavy reliance of a common man on Internet and computers urged the attention of State and non-State actors to intervene and exploit the weaknesses in Cyber Space.

In an article *"Pakistan and Cyber Crime: Problems and Preventions"* in 2019, Hamid Asmat analyses that it is the need of time to modify the existing laws on Cyber Crime and establish cooperation between International Community. He further explains that it is really hard to find the data about culprit from the computer and internet. Computer forensic is a new area and most of the countries are lacking its expertise and literature. Pakistan should adopt the proper laws and procedures about anti-Cybercrimes.

Extensive growth of Cyber Space in Pakistan

There were 87.35 internet users in Pakistan in January 2023. The number of web users in Pakistan increased by 4.4 million somewhere in between 2022 and 2023. The Internet penetration in Pakistan stood at 36.7% in January 2023. There were 71.70 million social media users in Pakistan in January 2023. (Kemp, 2023) There were 53.20 million users which are 18 and above in the start of 2023. As indicated by Pakistan Telecommunication Authority (PTA), the Mobile web infiltration is 191.8 million in 2023. The number of mobile connections in Pakistan increased by 5.9 million between 2022 and 2023. (Kemp, 2023) The sole entity that records and maintains demographic information in Pakistan is the National Database and Registration Authority (NADRA). Details on its citizens are crucial to Pakistan's battle against terrorist attacks. For its relevant functions, NADRA also provides the data to different government authorities. (Khawar, 2019) Due to its sensitivity, this data is vulnerable to theft and falsification. Cyber terrorism may now attack NADRA in an attempt to obstruct or disrupt its vital functions, steal private personal data, and utilise it for illicit ends.

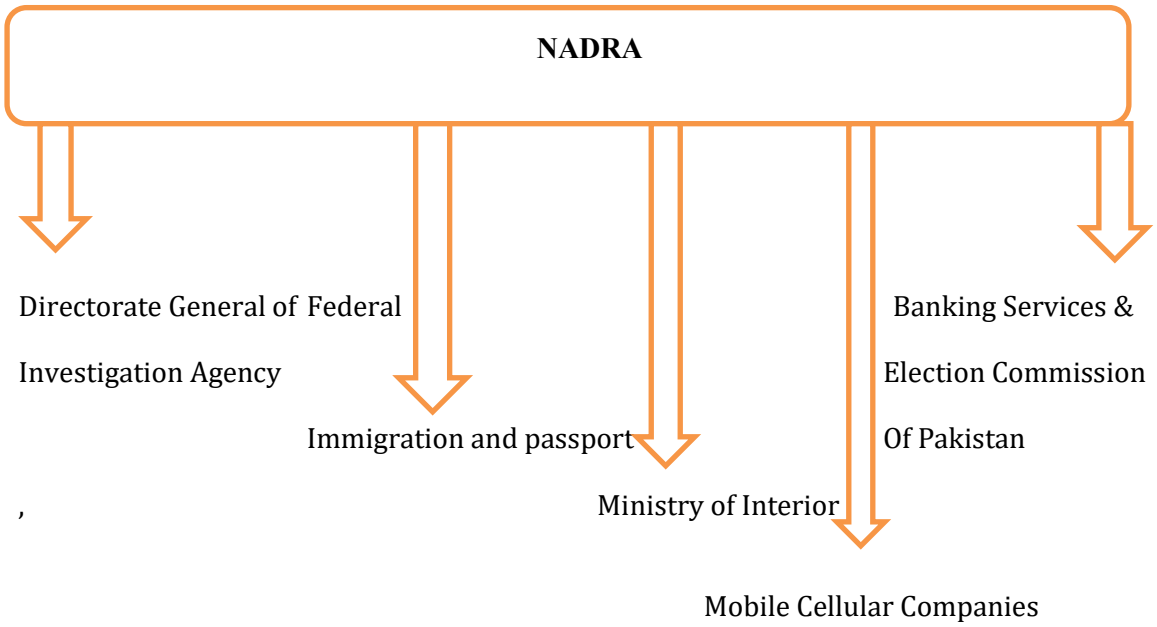

Figure: 1 NADRA and its important Services (Khawar, 2019)

The same is true for other IT-based businesses, such as banking services in Pakistan, where credit cards, account details, and other financial details can be obtained

for fraudulent or stolen purposes. The number of banking customers in Pakistan is rapidly growing, and with it, the risks that arise. The capital markets are economic marketplaces where long-term loans or investments are bought and sold. By shielding them against deception, these financial markets assist governments and organizations in investing their funds. (Khawar, 2019) The financial markets have evolved into computerized trading platforms in recent years. These trading networks comprise government agencies, investment firms, stock exchanges, and treasury agencies.

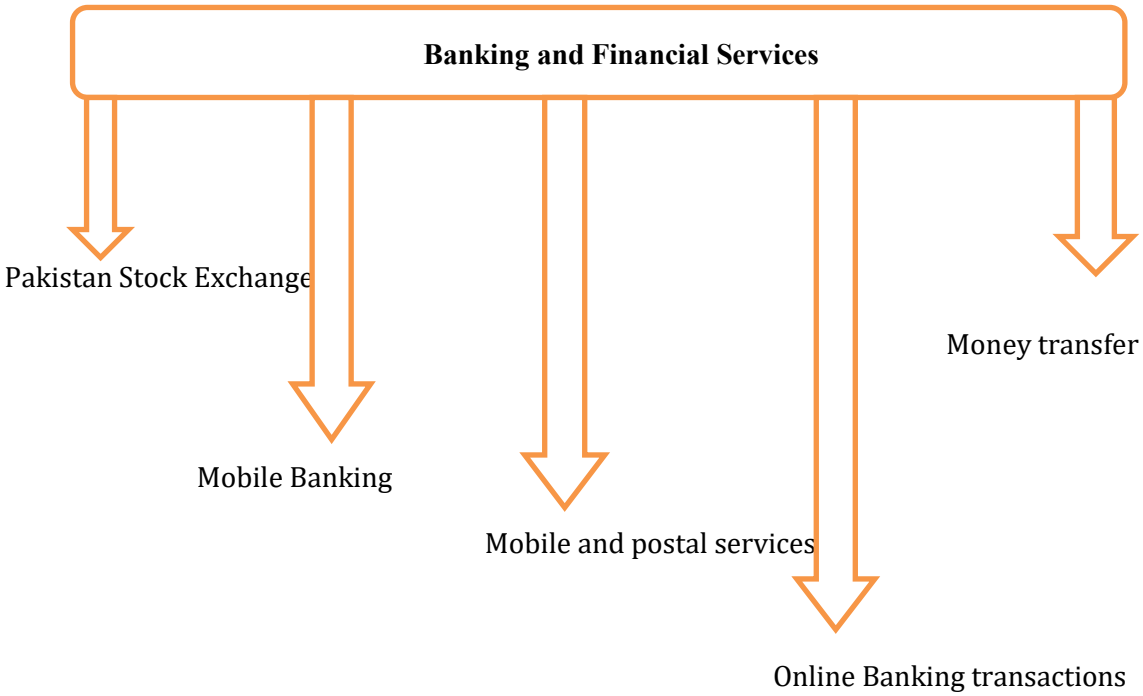

Figure: 2 Pakistan's Business and Financial Services (Khawar, 2019)

This massive existing usage of information and communication technologies, unlocked a new domain of Security known as Cyberspace. Now in this scenario, there should be awareness in general about the dangers of digital structures and about the part which they can play to ensure security. When this preparation is done, then, at that point setting up technologies and methodology to help these become simpler and more effective. According to the Global Cyber Security Index, Pakistan is ranking on 79th in 193 countries. According to researcher Rafay Baloch the current Cyber law "Prevention of Electronic Crime Act" is not properly implemented. For instance, Pakistan still has to develop its Cyber forensic laboratory, which can deliver a professional skilled view of the picture to law court free from inspective organization which is instructed in section 40 of PECA, Likewise, in section 49 of PECA, Central governmental authority has to entitle national and sectoral CERTs to protect national Cyber setup." (Emma, 2021)

According to the Microsoft Malware index of Asia pacific 2016, Pakistan is more vulnerable to Malware attacks and ranking at number 1. Indonesia, Bangladesh, Nepal are at second, Third and fourth positions whereas India is at eighth position. Pakistan is mostly encountered by three Malware families, Gamarue, Skeeya and Peals, which can steal the personal information, download more Malware and give access of your PC to hackers. (Microsoft, 2016) Recently in August 2021, there is a Cyber-attack on FBR (Federal board of Revenue, Pakistan), which resulted in the loss of taxpayers data from records. On 25th August 2021, The FBR data center was temporarily closed down for the recovery of taxpayer's data. According to the sources, an Irish company and Tania Aidrus have been assigned to examine the FBR'S data center and suggest ways and means to

ensure foolproof safety protocols. (Business Recorder) This situation has opened up a new domain of Cyber warfare.

Major Cyber Sectors of Pakistan:

The main cyber sectors in Pakistan are:

The Financial Sector: The main targets are frequently banks and other financial firms. Ransomware, phishing, and malware are among the online assaults that commonly target this industry. (Profit, 2024) The banking industry in Pakistan had a 114% rise in cyber-attacks in 2024, including ransomware, phishing scams, and fiscal viruses. Lazarus and SideWinder, two Advanced Persistent Threat (APT) organizations, have been especially active. (Profit, 2024)

Telecommunication: Cyber security has advanced significantly in the telecom industry because to programs like National Telecom CERT and the National Telecom Security Operation Centre (SOC). In 2023, the Pakistan Telecommunication Authority (PTA) documented a notable increase in cyber-attacks, such as 200 ransomware incursions, 300 Distributed Denial of Service (DDoS) events, 720 malware assaults, and 550 phishing attempts. (ProPkstaff, 2024)

The military and the government: These industries are particularly vulnerable to identity theft and online spying. Governmental systems and military figures have been the targets of well-publicized cyber-attacks. Millions of taxpayer's information was compromised in a significant cyber-attack that shut down the FBR for many hours. (ProPkstaff, 2024) The hackers sold the data that was taken on a Russian website.

Medical Care: Cyber-attacks can interrupt operations and jeopardize confidential patient information in the healthcare industry. (ProPkstaff, 2024) Major security risks were recorded in 2023, indicating that APT organizations were going after the healthcare industry.

Production/Manufacturing: Industrial cyber-attacks have the potential to severely interfere with supply networks and output. Ransomware and APT organisations have targeted important sectors in the industrial sector, resulting in cyber extortion tactics. The industry continues to be extremely susceptible to cyber-attacks. (ProPkstaff, 2024)

Challenges, Risks and Threats to Pakistan Cyber space:

Numerous dangers, hazards, and difficulties affect Pakistan's cyberspace and have the potential to affect its financial system, society, and national security. These are some important points.

Online Criminal Activity (Cyber Crime): Pakistan is vulnerable to a number of cybercrimes, such as malware assaults, monetary fraud, identity theft, and espionage. (Shad, 2019) Such offences may interfere with businesses, steal significant data, and inflict monetary damages

The act of cyber terrorism: Pakistan's essential facilities, including internet connections, transport networks, and energy infrastructure is seriously threatened by the threat of cyber terrorism. (Shad, 2019) Assault on such networks has the potential to cause fear and significant interruption.

Espionage via Cyberspace: Foreign actors frequently attack governmental agencies, military installations, and private businesses in state-funded digital spying in an effort to obtain strategic benefits and steal confidential data. (Rafique, 2019)

There is a warning issued by Pakistan's Senate Foreign Affairs Committee regarding Country's critical exposure to foreign Cyber-attacks and recommended that government should put more efforts in protecting Cyber boundaries of Pakistan by building up Cyber research and development centers. There is no organization working on Cyber Security in Pakistan whereas other countries like Israel and USA have their respective agencies CISA and NSA for the protection of their National security. The usage of borrowed technology from other nations is one of the more concerning issues that has sparked concerns about Pakistan's cyber security. It is reliant on technologies that are taken. Advanced countries provide, produce, and trade portals and various software and hardware IT equipment utilized by Pakistan. It is also one of the causes of the insecurity of Pakistan's internet. According to Pakistan National Cyber Security Policy 2021, Pakistan is lacking in Cyber skills, depending on foreign technology, having less resources, there is high level of deficiency in inter-departmental coordination, and lack of ownership at top level which makes Pakistan National Security vulnerable to Cyber-attack.

Cyber security as threat to Pakistan's National Security

The preservation of electronic networks and advancements in digital safety are largely dependent on national security. As a result, it is challenging to implement the digital retaliation plan, which is often a crucial tactic in traditional warfare. In efforts to counter Cyber threats different countries are strengthening their capacities, spending money on Cyber offensive and defensive equipments, hiring technological specialists, implementing preventive measures and setting up military commands for cyber operations. The importance of Cyber security cannot be disregarded in the current scenario of Communication infrastructure. In 10th International Conference on Cyber Security in 2018, Jeff Koseff stated that enhancing cyber security has two main advantages for national security: Firstly, it fortifies defense, lowering the danger of an attacker; secondly, it discourages assaults. Pakistan's national security is seriously threatened by cyber security for a number of reasons.

Vulnerability of Critical Infrastructure: Highly important infrastructure, including transportation systems, internet connections, and electricity networks, can be the target of cyber-attacks. When these systems are disrupted, it can affect national security and cause massive disorder. (Sahar, 2021)

Impact on the Economy: Businesses and economic activity might suffer serious economic harm as a result of cyber-attacks. As a result, the country's financial strength and, consequently, its national security may suffer. (Sahar, 2021)

Information collection and surveillance: Private armed and governmental information may be compromised by state-sponsored online spying. By revealing tactical intentions and eroding defense skills, this might compromise national security. (Sahar, 2021)

The act of cyber terrorism: Cyber terrorism offers an imminent danger by attacking critical systems, propagating disinformation, and inciting anxiety and dread among the populace. This might destabilize the country and cause security difficulty. (Adeel, 2021)

Database Violations: Identity theft, fraud, and other malevolent acts can result from unauthorised accessibility to confidential statistics, such as governmental documents

and confidential information, which can undermine public confidence and jeopardize national defense. (Government, 2021)

To protect Pakistan's national security from these dangers, a thorough cyber security plan, strong infrastructure, and continual surveillance are needed. Now today's Pakistan is leading towards technological innovations, information and computer technology system and e-government services. This move of Pakistan is entangled with the high risks of cyber security, and if those vulnerabilities are not addressed on time it can make ones present unstable and future disastrous because Pakistan is most snooped state in the globe. Not only India, many other countries including US are regularly spying upon Pakistan. According to report of Intercept US National Security Agency hired programmers and hackers to gain access in the VIP division of Pakistan Telecommunication Corporation which usually contain documents related to Pakistan's Civil and Military leadership. A programme known as SECONDDATE is said to spy on internet inquiries and reroute affected PCs browsing to an NSA website server. Internet queries are subsequently contaminated with virus by the server. (Dawn, 2016)

Indian Cyber Involvement in Pakistan:

On the other hand Pakistan archrival India under its Cold start doctrine is trying to engage Pakistan in Hybrid Warfare. This new form of warfare is nothing but intelligent employment of kinetic and non-kinetic warfare tools with relatively extra investment with regard to non-kinetic tools. Hurting economy; forcing change of regime; creating problems for armed forces; engineering inflation, unemployment, corruption; weakening state institutions, sponsoring terrorism and sowing discord among the adversary, are some of the important tools of hybrid warfare. (Minhas, 2019)Which can also be known as fifth generation warfare is a low-intensity conflict in which adversaries target each other's fault lines. (Minhas, 2019)

Indian government allocated 775 crores for Cyber security in 2015.They are not only working on the betterment of their Cyber Security but also using it against their traditional rival Pakistan. (Rafique, 2015)People of Pakistan are also not aware of the steps which they can take to secure their personal and official data from hacking and illegal access. Pakistan is lacking behind in technological advancement for the checking of Hacktivism. A lot of government, Military and banking sites were hacked by the hackers, one of the major example is the hacking of Pakistan FO websites in 2016. According to the spokesperson Muhammad Faisal, Pakistan's Army and Foreign Ministry websites were hacked on 16th February 2016 by India. This Cyber-attack was due to a terrorist strike at Palwama, Kashmir, which took the life of 40 Indian military personnel and the responsibility was taken by Pakistani based Jaish-e-Muhammad. (ecouncil.org) In 2020 Pakistan Security services discovered Cyber assault on Pakistan military and government officials' mobile phones by Indian intelligence agencies. Again in February 2021 by utilizing cellular monitoring equipment, a group of hackers known as Confucius, supported by the Narendra Modi administration, spied on critical areas in Pakistan and Kashmir. It attacked on almost 150 people in prominent positions within Pakistan armed forces, Atomic energy Commission and Nuclear Regulatory body. (Ahmed 2023) Pakistan was also victimized by the DDoS attack when State bank services were halted for 21 days in 2008. In 2018 banking industry was also targeted, when the data of 22 Pakistani banks were on sale on dark web. In December 2018 the ATM's of Habib bank were targeted. In May 2020, the Iranian hacking group Greenbug expressed intent on obtaining a hold on the computerized records of three telecommunications providers in Pakistan. (Ahmed 2023) Recently an APT organization Rattlesnake tried to steal confidential information from Pakistan Navy website. The power outrage of January 2023 also highlighted that how susceptible the national electrical infrastructure is to possible Cyber-attack although at first Ministry of Energy claimed that interruption was the result of technical malfunction but latter on a unique causative element has been found after similar case studies on

extended power system breakdown. Although extensive outages in the past were frequently ascribed to technical in nature, but a deeper look indicates that the latest occurrence may have been the consequence of a malevolent digital-attack. There the fundamental issue relates to online safety. (Salik, 2023) Pakistan Telecommunication Authority is a governmental organization to check and ban the illegal sites for the betterment of Cyber security but it fails to stop these sites properly. PTA blocked 15000 sites in 2012 and 13 but is not that much effective in banning YouTube which is the biggest failure and alarming situation for Pakistan's National Security.

Indian Partnerships with Israel and the United States:

Indian digital intrusions on Pakistan have become a more severe danger in light of India's growing cyber security partnership with Israel. Israeli Prime Minister Benjamin Netanyahu in 2019 while speaking to the global Cyber security Session emphasize on making Israel as major Cyber Security influencer in the globe. He further stated that In terms of Cyber Security they as a nation worked more than any other nation. Now because of Israel strong grip over Cyber Security matters, Indian Policy makers are looking toward the Israel's Talpiot training program which recruit most talented individuals form different countries and train them in Mathematics, Physics and Computer Science to produce Cyber Security experts. This is quite disturbing situation for Pakistan and they should take some serious measures and appropriate strategies to secure their private records or Institutional data Now in this Scenario Pakistan needs to build a solid Cyber Security framework to deal with stealing of economic records, Identity theft, and Observation of sensitive setup.

India's offensive digital interest is Pakistan-focused and "geographically efficient," rather than aimed at China, in spite of a "acute rise in Chinese activity towards Indian networked devices," based on a recently released study from the International Institute for Strategic Studies (IISS), a reputable research organistaion with significant rules clout. (Babar 2022) Greg Austin, who oversees the IISS's cyber program, claims that while India possesses certain attacking cyber and digital-intelligence skills, they are mostly directed at Pakistan. It is currently working to make up for its imperfections by seeking coordinated global efforts to create control guidelines and by creating improved novel abilities with the help of significant global allies like the United States, the United Kingdom, Israel, and France. (Babar 2022)

Measurements taken for Cyber space protection in Pakistan

To counter the digital threats the country is facing today, and for the betterment of national Digital safety situation, it is important to enhance state's Cyber Security abilities by developing a well-coordinated mechanism, implementing digital Security standards and to have a legal framework.

For this, government took an initiative in 2016, by passing Prevention of Electronic Crime Act (PECA) which recommends penalties for Cyber offenders. This act proposes fines and jail terms for those, involved in having an access of unauthorized information, unapproved plagiarism, access to any serious set-up, internet scam, alteration of communication evidences and having an offence against the persons modesty and civility, writing malicious codes and their transmissions, Cyber stalking, and involved in digital hate speeches. It further proposes the formation of Pakistan CERT which started working in 2000 with the name of PAK-CERT. It is the National Computer Emergency Response Team for Pakistan which provides assistance in identifying the intruder's activities, and Security compromises. Furthermore to create a cyber governance framework, Government of Pakistan has formulated first National Cyber Security policy-2021.

Inspite of all these efforts there are obviously recognizable obstacles in setting up a significant network safety design in Pakistan for example the absence of central authority to work on network protection issues and prompt the Prime Minister on arising digital dangers. There is a substantial absence of mindfulness inside the policymaking circles and no such bill instead of cybercrime bill which can be made as a strategy regarding the matter of Cyber safety. There is no obvious Characteristization of digital safety associates and in which territories they have to work are not appropriately clear. Currently Pakistan has no PK-CERT and there is no monetary reserves dispensed for the purpose of online protection. The National Examination Organization (FIA) has a National Cyber Response Center for Cyber Crime (NR3C) yet their order is restricted which cannot perform his duty to be the first one to respond to digital crisis situation. Pakistan is represented at the UN Group of Governmental Experts on Information Security (Crime), however public perspective communicated on these gatherings are not conveyed to people in general. There is no instrument which can provide understanding between states or which can share its best practice at regional basis. So a lot of work still needed to be done.

Conclusion

The specialty of war is certainly its ever changing pattern and an action in regards to how, when and where you can collaborate with your opponent. Universally there is an emergence of new risk is emerging not just for states but also for the privately benefit motivated world. Billions of dollars and pounds are unlawfully moved and taken, Privacies endangered, state systems and methods are bought and important critical setup hacked. That world is really known as the world with digital Crime. Today the whole realm turns out to be increasingly more connected by means of web or digitalized through information designing, the digital security threats are expanding step by step. The transnational idea of Cybercrime makes network safety a worldwide test and requests aggregate measures at the global level with immaculate Cyber strategy Frame work.

Pakistan isn't any special case for it. An atomic state having a fundamental international position is altogether exposed to such dangers in the digital domain. Pakistan incorporates an enormous web client’s base, expanding web insurance tools and banking measures which rely upon web connected networks. Now in this Scenario Pakistan needs to build hard-hitting Cyber Security Structure which can strongly deal with mugging of economic statistics, Identity theft, and Observation of sensitive setup. Furthermore there should be an enactment, policy making, organized efforts, and aggregate liability to have a secure Cyber space for Pakistan.

Recommendations

The public authority needs to put resources into modernizing its organizations to empower them to manage digital threats. Currently there is no such organization in Pakistan which deals with its online protection. Country requires an undisputable office for defending it from digital assaults e.g., the United States has the Cybersecurity and Infrastructure Security Agency (CISA) and Israel has Unit 8200 or the National Cyber Security Authority (NCSA). In Pakistan, the National Response Center for Cyber Crime (NR3C), a unit of the Federal Investigation Agency (FIA), manages cybercrimes; but it’s not able to completely safeguard Pakistan’s sensitive information and is lacking in assets, labor and offices as well.

Pakistan likewise needs adequate law for dealing digital dangers. In 2016, Pakistan passed a cybercrime law called the Prevention of Electronic Crimes Act, 2016; but that law doesn't cover numerous vital parts of cyber protection. Pakistan needs more significant network safety guidelines which can help organizations and associations to shield their Cyber security frameworks and data to become a victim of digital assaults. There should be guidelines which command government division, power division, and medical care,

monetary organizations to shield all digital frameworks or data to be penetrated. These procedures remain significant because all organizations are currently associated with the web and are becoming more reliant upon AI (Artificial Intelligence). This makes them an easy access for hackers. Whereas cyber safety specialists, claims that organizations are not focusing on online protection unless the pressure is not coming from the government.

There should be a deep understanding in Pakistan about a desperate threat to its sensitive set-up and it must put forth hard and fast attempts to guarantee the safety of connected infrastructure of Pakistan. As a whole, it's significant for Countries legislators to categorize immediate & upcoming digital dangers and figure out network safety procedure as early as possible. Pakistan cannot give assurance about complete public and economic safety without viably handling these virtual threats.

References

Awan, J., & Memon, S. (2016, March). Threats of cyber security and challenges for Pakistan. In 11th International Conference on Cyber Warfare and Security: ICCWS-2016*, Boston USA (p. 425).*

Baloch, H. (2016). *Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016.* Accessed on 23rd June.

Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, 42(5), 495-499.

Broadhurst, R. (2006). Content cyber-crimes: criminality and censorship in Asia*. Indian J. Criminology,* 34, 11.

Fischer, E. A., Liu, E. C., Rollins, J., & Theohary, C. A. (2013). *The 2013 cyber security executive order: Overview and considerations for congress* (pp. 7-5700). Washington: Congressional Research Service.

Furnell, S. (2003). *Cybercrime: Vandalizing the information society.* London: Addison-Wesley.

Furnell, S. (2003, June). *Cybercrime: vandalizing the information society. In International conference on web engineering* (pp. 8-16). Berlin, Heidelberg: Springer Berlin Heidelberg.

Goldman, D. (2012 September). Major Banks hit with biggest cyber-attacks in history*. CNN Money.*

Grabosky, P. (2004). *The global dimension of cybercrime. In Global Crime Today* (pp. 146-157). Routledge.

Haq, Q. A. U., & Atta, Q. (2019). Cyber security and analysis of cyber-crime laws to restrict cyber crime in Pakistan. *International Journal of Computer Network and Information Security*, 11(1), 62-69.

. Holt, T., Bossler, A., & Seigfried-Spellar, K. (2022). *Cybercrime and Digital Forensics: An Introduction (3rd ed.).* Routledge. https://doi.org/10.4324/9780429343223

Hui, K. L., Kim, S. H., & Wang, Q. H. (2017). Cybercrime deterrence and international Legislation*. Mis Quarterly*, 41(2), 497-524.

Iqbal, Z., & us Shan, R. (2024). Pakistan's Cybersecurity Landscape*. CISS Insight Journal*, 12(2), P105-131.

John, M. (2011). Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*, 2.

Khawar, R. S. (2019, February*). Cyber Security: Where Does Pakistan Stand?* . Retrieved from sdpi.org: https://sdpi.org/sdpiweb/publication

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives.* Springer Science & Business Media.

Kundi, G. M., Nawaz, A., Akhtar, R., & MPhil Student, I. E. R. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries*. Journal of Information Engineering and Applications,* 4(4), 61-71.

Manzar, U., Tanveer, S., & Jamal, S. (2016). *The incidence of cybercrime in pakistan.* Researchgate.net

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Summary of key findings and implications. *Home Office Research report*, 75, 1-35.

Momein, F. A., & Brohi, M. N. (2010). Cyber crime and internet growth in Pakistan*. Asian Journal of Information Technology,* 9(1), 1-4.

Moran, G. (2014). We Are Anonymous: Inside the Hacker World of LulSec, Anonymous, and the Global Cyber Insurgency*. Journal of Information Ethics*, 23(2), 95.

Mushtaque, K., Ahsan, K., Nadeem, A., & Umer, A. (2014). Critical Analysis for Data Privacy Protection in Context of Cyber Laws in Pakistan*. Journal of Basic and Applied Scientific Research,* 4(10), 1-4.

Pladna, B. (2008). *The Lack of Attention in the Prevention of Cyber crime and How to Improve it. East Carolina University* [Online] available from< http://www.infosecwriters. com/text_resources/pdf. BPladna_Cybercrime. pdf>[April 30, 2011].

Putnam, T. L., & Elliott, D. D. (2001). *International Responses to cyber crime.* Transnational Dimension of Cyber Crime and Terrorism*,* 35-66.

Rasool, S. (2015). Cyber security threat in Pakistan: Causes, Challenges and Way forward*. International Scientific Online Journal*, 12, 21-34.

Rehman, T. U. (2020). International cooperation and legal response to cybercrime in Pakistan. *In Encyclopedia of Criminal Activities and the Deep Web* (pp. 424-434). IGI Global.

Sadeleer, A. S. (2012). *Cyber Security in the European Union: An Integrated Defense Strategy for 21st-Century Warfare?.* Cyber Security in the EU.

Ashraf, S. (2021). Geopolitics of Climate Change: US and China are Reciprocal Contenders. *Journal of Development and Social Sciences,* 2(3), China-Climate.

Tariq, M., Aslam, B., Rashid, I., & Waqar, A. (2013, December). *Cyber threats and incident response capability-a case study of Pakistan.* In 2013 2nd National Conference on Information Assurance (NCIA) (pp. 15-20). IEEE.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society.* Torrosa.com

Zahoor, R., & Razi, N. (2020). Cyber-crimes and cyber laws of Pakistan: An overview. *Progressive Research Journal of Arts & Humanities* (PRJAH), 2(2), 133-143.