ns **Seminar Paper**

Title: **Role of Pakistan in cyber warfare: State-Sponsored attacks and Defense Strategy**

Zainab Chaudhary

Abstract:

This paper will analyze the areas of Pakistan's participation in cyber warfare from 2010 to 2023, focusing on the state-sponsored alleged cyber operation and its changing defense policies. With the digital technologies taking center stage in national security, states are starting to utilize cyberspace in strategic signaling, data collection, and infrastructure disruption without necessarily engaging in military conflict. The cyber role of Pakistan is influenced by the regional geopolitical pressures and the fast development of both the public and the private networks into digital space. The most important instances that are often subject to research are the claims of cyberattacks on Indian government systems and the general issue of ensuring that Pakistani digital infrastructure is also secure. The strategic approach of Pakistan involves adopting national cybersecurity policy frameworks, legislations and building institutional competencies to safeguard the critical sectors. The study places the cyber posture of Pakistan in the international and regional contexts of cybersecurity, with opportunities and challenges arising in resilience building. It throws light on the policy frameworks and the collaborative action to augment cybersecurity governance and pushes the necessity of joint actions by the policymakers, technologists, and actors of civil society. The results add to the idea of how states such as Pakistan cope with cyber threats as an element of strategic statecraft to reveal the significance of multidimensional defense structures in ensuring national security in an interconnected digital world.

Introduction:

Cyberspace has become one of the most important spheres of strategic, economic, and political relations between states in a fast-changing digital age. Contrary to the conventional theater of war, which is limited by geographical and military logistical factors, cyberspace provides a big and relatively borderless space on which states can exert influence, collect intelligence, cripple rivals, and indicate strategic intentions without necessarily using military force. According to the scholars, the digital world is where the boundary between civilian and military infrastructure becomes unclear, and a hybrid ecosystem is formed where the instruments of espionage, sabotage, and propaganda are inextricably mixed with the civilian technological one.

To Pakistan, this change is of special importance. Being placed in a geopolitically sensitive area and experiencing long-term strategic rivalry with its neighbors, Pakistan has more and more noticed cyberspace as a hope and a threat. The growth of the digital networks of the public institutions, financial systems, telecommunications, and infrastructure has increased the vulnerability of the country to cyber threats. At the same time, these networks provide

the state with an opportunity to acquire defensive capabilities, seek strategic deterrence, and digital diplomacy. The dual nature of cyberspace as the possible war front and the means of empowering the nation, highlights the significance of cyberspace in the national security calculations of Pakistan.

The analysis of the role of Pakistan in cyber operations consequently gives useful information in how a developing state in the contemporary world manages the intricacies of digital warfare. Although the global powers might spend a lot of resources on cyber militarization and offensive capabilities, the developing nations such as Pakistan, tend to work with resources, technical and institutional maturity limits. However, strategic imperatives, regional security issues, and the demands of national sovereignty lead to the establishment of consistent policies, laws and operational capabilities.

The proposed research will examine the development of Pakistani cyber posture since 2010 and 2023, a decade characterized by the growing significance of cyber threats, as well as institutional response to them. The paper highlights the supposed cyber operations that are linked to state actors and the measures that Pakistan has established to protect its networks. Through these two dimensions, the study places Pakistan in the larger framework of discussing international cybersecurity, which states strike a balance between the offensive and defensive aspects of cyber strategy.

The importance of the current research is that it bridges various academic views. It combines the knowledge of international relations theory, the research of cybersecurity, and the strategic analysis of policies. The realist approach explains the incentives of cyber activities as an instrument of power projection, whereas constructivist ideas explain the perceptions, norms, and threat discourses in influencing policy reactions. The institutional aspect is also taken into account to assess how policies, legislative frameworks, and functioning bodies can interrelate to influence the resilience of a country in the field of cyber.

Through the consideration of a qualitative method based on documentary analysis, policy review, and secondary research, the study explores the major trends, patterns, and issues in the cyber world of Pakistan. This methodology enables the analysis of each of the strategic rationales as well as institutional capabilities in detail, thereby giving a holistic picture of which processes drive cyber engagement. It also brings out the interaction between the internal policy formulation and the external geopolitical factors as a way of establishing the cyber strategy of Pakistan in the overlay of the South Asian region security dynamics. The study highlights the essence of cyber governance as a key element to national and regional security. The growing interdependence of the economic, political, and technological systems makes effective cybersecurity no longer an outlining issue but a part of the national strategy. Through comprehending the policies, difficulties, and institutionalization of Pakistan, in this field, scholars, policymakers, and practitioners of security can be enlightened on evolving

dynamics of cyber conflict within developing states, the issue of threat attribution, and how risks in the rapidly evolving digital space are being reduced.

Significance of Research:

The study will be of importance to policy makers, cybersecurity workers, and international security scholars in government. The development of cyber capabilities and the strategy of Pakistan can help in the analysis of a threat better, making policies, and developing comparative studies on the dynamics of cyber conflict in volatile regions.

Motivations:

The study is inspired by scholarly concerns with cybersecurity, geopolitics, and national security. With the cyber operations now appearing as an element of the state strategy, exploration of the role of Pakistan in the scope of cyber warfare offers a perspective into the overall trends in cyber warfare in the region and the world.

Limitations:

The major weakness of the research is the lack of publicly verifiable data on cyber operations and defense strategies because cyber activities have turned out to be a clandestine operation, and the lack of access to classified information. Issues of attribution also make accurate judgments difficult. The qualitative mode helps to counter these problems by emphasizing written records of policy and valid analysis.

Research Objectives:

The aims of the study are to:

- Investigate Pakistani state-backed cyber operations 2010-2023.
- Evaluate the cyber defense strategy of Pakistan.
- Find main issues and opportunities to enhance national cybersecurity.

Research Questions:

1. How efficient are the national cyber defense regulation systems in facing government-supported cyberattacks?
2. What are the main challenges and opportunities that Pakistan has to improve cybersecurity?

Literature Review:

The sphere of cyber warfare has also expanded tremendously, with digital technologies forming the foundation of state security, economic infrastructure, and governing structures. The use of cyber operations as a means of espionage, sabotage, disinformation, or attacks on critical infrastructure proves the multidimensional character of modern conflict. The

recent academic sources emphasize the fact that cyberspace has expanded the national security domain to allow it to transcend geographical boundaries.[1]

The strategic rivalry between Pakistan and India in the South Asian context has gone digital. Researchers point out that cyber incidents among the two states tend to be a mirror of the presence of geopolitical tensions, where the networks, communication systems, and other critical services of the state are the targets of the hostile actions, and policy responses and defensive stances to such actions are shaped through the strategic framing of cyber threats.[2] Although such attacks are usually difficult to pinpoint, the literature notes that such activities are strategically framed as a national security concern that results in policy responses and defensive postures by both states.[3]

The literature also talks about national cybersecurity governance structures. The policy approach to dealing with cyber threats is multi-stakeholder-based, with the National Cyber Security Policy 2021 being a structured document that offers resilience in the realms of the public and the non-governmental sectors, with an emphasis on governance, technological capability, and inter-agency coordination and collaboration.[4]

Scholars observe that the cybersecurity environment in Pakistan continues to face some challenges, such as the lack of technical capacity, insufficient resources, and inadequacies in terms of implementing the policy measures.[5] On the whole, the literature indicates that the involvement in the area of cyber warfare in Pakistan is indicative of the wider state-level attempts to cope with the changing digital threat, juggling between strategic needs and institutional constraints.[6] The interaction of policy, legal framework, and institutional capacity illustrates the difficulty of developing a holistic cybersecurity posture in a geopolitically competitive region.

Literature on cyber deterrence is also divided at the strategic level. Other researchers propose that believable defensive capability and strength are effective deterring measures because they decrease the payoffs of attack. There is an argument by others that attribution issues weaken deterrence credibility. The debates on deterrence in the Pakistani context are defined by the regional security issues as well as by the South Asian strategic culture. Although the discourse of official policies focuses on defensive preparedness, scholarly debates often focus on the impact of regional competition on cyber threat perception. Another main theme in the scholarship of cybersecurity is international cooperation.

---

[1]Sara Ahmad, “Cyber Security Threat and Pakistan’s Preparedness: An Analysis of National Cyber Security Policy 2021,” Pakistan Journal of Humanities and Social Sciences Research 5, no. 1 (2022). ([ResearchGate][4])
[2]Jannat Naseeb, “Framing the Digital Threat: Cybersecurity and Strategic Narratives in India-Pakistan Relations,” International Journal for Conventional and Non-Conventional Warfare (2025). ([researchcorridor.org][5])
[3]Ibid. ([researchcorridor.org][5])
[4]Government of Pakistan, National Cyber Security Policy 2021 (Ministry of Information Technology & Telecommunication, 2021). ([MoITT][1])
[5]N. Shabbir et al., “Cyber Security: A Growing Challenge to Pakistan,” (2025). ([ojs.ahss.org.pk][6])
[6]National Cyber Emergency Response Team (PKCERT) and National Cyber Crime Investigation Agency (NCCIA) official descriptions. ([PKCert][7])

Normative development and technical cooperation are facilitated by multilateral forums, agreement of information sharing and involvement in international cyber governance talks. Capacity-building projects and cross-border training are usually useful in developing states. As in the case of Pakistan, participation in the international cybersecurity dialogue gives them an opportunity to share their knowledge and build strategic confidence but at times the geopolitical complexities restrain the level of cooperation. The literature acknowledges the dynamic characteristics of cyber threats. The threat landscape is constantly changing due to the emergence of new technologies in the form of artificial intelligence, automation, and sophisticated malware. It follows that adaptive governance mechanisms are required in order to provide long-term resilience. Researchers warn of fixed policy architecture and promote the use of repeated reforms in response to the changes in technology.

To conclude, the literature that is available places the development of cybersecurity in Pakistan in the context of a wider global trend of cyber militarization and institutional reformation and the expansion of digital governance. Although the nation has made some significant steps in the development of policy frameworks and institutional capacity, there still exist some challenges in terms of implementation, expertise, and the dynamic nature of the threats. The role of cyber warfare in examining the role of Pakistan is based on the intersection of geopolitics, technological change, and institutional development in the country.

Theoretical Framework:

Looking at the assumptions made and the approach taken to the research suggested here, one can say that the theoretical basis of the proposed research appears to refer both to Realism and Constructivism. According to realism, nation-states fight cyber warfare to realize their goals in the strategic domain and as a form of providing national security. This theory posits that states undergo cyber conflicts, particularly Pakistan and India in this scenario, since such conflicts are strategic conflicts that are supposed to offer a solution to strategic problems that afflict a region in an effort to attain objectives. Constructivism, on the other hand, concentrates on cultural, social, and interactions among the members of the group in the perception and management of threats in cyberspace. To begin with, Constructivism means that the images of various societies and, as a result, the state attitudes, beliefs, and norms determine concepts of cyber warfare and how states respond to new cyber threats. In this regard, it is in this context that the paper attempts to analyze how and why Pakistan uses and defends the cyber-space in international relations, the nature and roles of cyber warfare the country has been engaging in, and the types of cybersecurity policies that the country has undertaken.

Research Methodology: The peculiar approaches of this research mission aid in the comprehensive analysis of the cyberwar in Pakistan, with a particular focus on the defense and defense techniques introduced by the state. The qualitative research that is going to be used seeks to examine the extremes of cyber conflict in South Asia. It achieves this by

examining the diverse forms of data sources and analysis procedures available and deriving information that discusses not only the capabilities of cyber in Pakistan but also the problems associated with them. This chapter shows the research design, data collection process, analysis process, limitation and ethical considerations as well as the conclusion of this mark by methodology rationale.

Since this research employs the qualitative research methodology, which allows collecting the data on the complex topics, such as cyberwarfare, the present study is dedicated to this mysterious field. The qualitative methods also enable a deep infiltration into the contextual dynamics, themes and implications of digital practices in Pakistan but the overall outcome is a subtle understanding of the environment of cyber in Pakistan. Through the literature review, documentary analysis, and interviews with the experts, this study will develop a holism concept of the situation of cyberwarfare in Pakistan during the identified period.

The basic instruments of this study are the documentary analysis that will be applied in the course of the research work. official paperwork, records, policies, and academic books represent the most valuable sources of information, they make facts about the Pakistan policies online, cases and the defense strategy. The documentary analysis involves, the act of critical systematic investigation of the text data that provide the researcher with the capacity to recognize the perspectives in existence, patterns and any incongruence in the cyber narrative of Pakistan. In addition, the dissimilar secondary data sources (e. g. news articles, thinking programs, reports of international organizations) also prove useful to make the analysis complete. Besides, the various points of view are pointed out in the documentary analysis.

The data that is used to collect information in this study is in the form of various sources including academic data bases, the government website, online archives and information repositories. The main sources of data can be deduced by the data produced by the Governmental bodies of Pakistan and the agencies of cybersecurity and the foreign bodies where they are granted. Which provide an insight into the cyber policies, the incidents, and the defense mechanisms that Pakistan has and provide a solid basis on which to base on when explaining the cyber environment in the country. The origin of secondary information - the scholarly articles, news reports, analysis of think tanks and opinion of the specialists regarding the cyber activities of Pakistan, give fresh insights and more discoveries although it might sometimes distort the truth. With the help of the vast data acquisition process, the basis of this investigation is, therefore, reinforced and later beverages to the comprehensive analysis of the associated findings.

This analysis takes a thematic approach. Documentary sources are coded, categorized and organized qualitative information. By the way of abductive approach to logic recurrent themes, patterns, and trends are determined. The thematic analysis will help in the systematic study of the data, summarize the right conclusions made and find the common grounds amidst the many aspects of the cyber conflict of Pakistan. The procedural

component of analysis process will consist of organizing data and themes, developing a coding guide or key points and coming up with conclusions that will form a basis of developing a coherent narrative about the cybersecurity of Pakistan. During the processes of critical analysis, the research will be in a position to make significant conclusions and recommendations that will help clarify the real nature of the cyber warfare being fought by Pakistan.

There are a number of limitations that should be considered in this research. To begin with, some factors such as the secrecy of the government, no authority to some secretive information, and the inconsistency of the cyber acts may restrict the availability and credibility of the information on the cyber activities in Pakistan. There is also the limitation of the research to the readily available sources that might not reflect or reveal the full picture of cyber capabilities and actions of Pakistan. Similarly, personal perception of the data and the potential biases that a researcher might present can also be a source of skewness, which can bring the analysis and the ultimate conclusions derived from the study to bias.

The most pertinent argument in undertaking research on cyber warfare is the issues of ethical concern due to the nature of the topic being sensitive and potentially harmful to national security. The research self-administers ethic guidelines of informed consent, confidentiality, and a lot of respect towards the autonomy of the participants. Instead of the study being founded on primarily individual sources, this concern is intimate given to the ethical standards. However, the effort is done in making sure that the data is utilized appropriately, all the references to all the sources are provided with accurateness of claims, and no false information is provided.

Part 1

Introduction: The advent of cyberspace as a strategic space has radically changed the character of contemporary conflict. The twenty-first century is marked by the fact that states are increasingly depending on digital infrastructure to govern, communicate, and have financial systems, as well as coordinate their military efforts. Consequently, cyberspace has become a battleground where rivalry, espionage, and political signaling take place without having to fight on the battlefield.

To nations that experience recurrent security dilemmas, cyber capabilities are an added tool of statecraft. Pakistan is in a geopolitically sensitive place, and the country has been involved in a long-standing rivalry with India; hence, it has slowly realized that cyberspace is both its weakness and its asset. The rapid digitalization of state institutions and critical infrastructure

has increased vulnerability to cyber threats and, at the same time, raised the strategic significance of cyber defense.[7]

This paper analyses Pakistan's involvement in cyber warfare since 2010-23 in two key aspects: purported state-sponsored cyber activities and cyber defense policy formulation by the nation. It will not seek to pass unproven propositions, but it is aimed at interpreting reported cases, policy history, and institutional reaction on a wider regional and theoretical basis.

Analysis of State-Sponsored Attacks: Claims about state-sponsored cyber activity have become a common element of the South Asian security discourse. The area and world have been concerned with cyberattacks that have been linked to entities associated with Pakistan, especially regarding the tension between India and Pakistan.[8]

A very publicized example here was the case of 2012, when a series of Indian government websites were brought down temporarily due to cyberattacks that were attributed to Pakistani cyber attackers. These actions mostly entailed defacing websites and distributed denial-of-service (DDoS) methods, although concrete attribution continues to be a contested topic.[9] The episode demonstrated that during times of diplomatic tensions, political signaling and using cyber tools as a method of symbolic retaliation can be employed.

In 2016, the hacking of websites and defacing of Indian websites were claimed by the groups who identified themselves as the Pakistan Cyber Army. These events indicated that the distinctions between state and non-state cyber operations in regional conflicts are not so clear, even though the level of coordination between such non-state actors and the Pakistani state is not well understood.[10]

The other significant cybersecurity issue arose in 2018, when mass disruption to power occurred in Pakistan. Although technical inspections conducted later pointed at the failure of both the system and the transmission instead of the fact of actual foreign cyber sabotage as the main cause of the blackout, the event heightened the urgency of enhancing cyber resilience.[11]

These examples show that there are three key trends:

1. The growing application of cyberspace in strategic messaging.
2. The challenge of being able to categorically assign cyber incidents.

---

[7] Ministry of Information Technology and Telecommunication (Pakistan), National Cyber Security Policy 2021, Government of Pakistan.

[8] Sameer Patil and Anirudh Kanisetti, “Cybersecurity in South Asia,” Observer Research Foundation, 2019.

[9] “Indian Government Websites Hacked by Pakistani Group,” The Times of India, December 2012

[10] “Pakistan Cyber Army Claims Attack on Indian Websites,” BBC News, September 2016.

[11] Salman Masood, “Pakistan Power Outage Plunges Country Into Darkness,” The New York Times, January 9, 2021 (discussing infrastructure vulnerabilities and blackout causes).

3. The fact that critical infrastructure is becoming more vulnerable in states that are digitally reliant.

South Asia Cyber conflict represents the global trends of digital supplementing conventional strategic competition.[12]

Defense Strategies: To address such new cyber threats, Pakistan has made efforts to institutionalize its cybersecurity governance framework. The fact that national policies and legal frameworks have developed indicates that cyber threats have become a national security concern.[13]

Legislation A legislative foundation for dealing with cybercrime and unauthorized access to digital content was offered in the Prevention of Electronic Crimes Act (PECA) 2016. More recently, the National Cyber Security Policy 2021 established a methodical perspective towards dealing with critical information infrastructure, enhancing institutional coordination, and the development of technical capacity.[14]

International cooperation has also become a necessary element of the governance of cybersecurity. Pakistan is also working hard to keep pace with changing global standards in cyberspace, which can be seen through its participation in multilateral meetings on responsible state conduct on cyberspace.[15]

Comprehensively, the cyber trend in Pakistan shows a slow adoption of cyber defense systems and constant cyber conflicts in the region. Its cyber posture is still influenced by the convergence of geopolitics, technology, and national security.

Part 2

Analysis of State-Sponsored Attacks: This chapter focuses on cyber incidents and trends in 2010-2023 directly or indirectly connected with the actors related to Pakistan. At the very beginning, it is necessary to explain that cyber attribution has become one of the most disputable questions of international security. Numerous cases are founded on technical evaluations, intelligence conclusions, or media checks as opposed to governmental confessions. This section as such will examine trends, reported infections, and larger strategy trends as opposed to unverified charges.

The cyberspace has become the competition field of states in the past decade. There have been sporadic cyber tensions in South Asia, especially in India and Pakistan, which are a reflection of the geopolitical conflict in real life. According to scholars, the cyber operatio

[12]Lucas Kello, The Virtual Weapon and International Order (New Haven: Yale University Press, 2017).
[13] Government of Pakistan, National Cyber Security Policy 2021.
[14] Government of Pakistan, Prevention of Electronic Crimes Act (PECA), 2016.
[15] Ministry of IT & Telecommunication, National Cyber Security Policy 2021.

within this region tend to be more of the signaling/retaliation/symbolic projection of power than all-out cyber warfare.[16]

The cyber environment in Pakistan should be perceived in the context of the overall security environment in Pakistan. The persistence of territorial claims, the distrust between the countries in the region and the traditional military rivalry, have influenced the digital interactions between the conflicting states. Cyber incidents, in most instances, are accompanied by political crises or tensions on the border, implying that there is a tendency to increase digital confrontation along with physical confrontation.[17]

2010-2013: Early Digital Confrontations: The 2010-2013 period was an initial stage of observable cyber antipathy enacted by India against Pakistan. Over the period, several Indian government websites were vandalized by hacker organizations purporting to be part of Pakistani causes.[18] This was usually done through Distributed Denial of Service (DDoS) attacks or through symbolic website defacements with political slogans.

It is however important to differentiate on the state sponsored operation and the hactivist activity. Lots of these initial attacks were done by organizations including the "Pakistan Cyber Army" which publicly described itself as ideologically motivated but was not actually state-controlled.[19] Indian authorities usually accused indirect government assistance, but there is very little actual evidence that it was a state organization.

Cyber conflict scholars refer to this point of time as low-intensity cyber rivalry, or digital actions were mostly symbolic and psychological and not destructive.[20]

2014-2016: Escalation and attribution Challenges: Cyber incidents became common and more politicized between 2014 and 2016. There were reports that Indian military and government affiliated websites were attacked by hacker groups which were allegedly based in Pakistan at times of high tension between the two countries.[21]

The attribution at this era became more intricate. Cybersecurity analysts pointed out that the nature of cyber operations is based on a practice of proxy actors, spoofed digital signatures, and false flag procedures. According to Thomas Rid, cyber attribution demands high standards of evidence and seldom attains the level of certainty that is found in the courtroom in the general public.[22]

It was also noted by the international observers that India and Pakistan accused one another of cyber intrusions and showed no proof of convincing the world of such actions. This two-

---

[16]Joseph S. Nye Jr., The Future of Power (New York: PublicAffairs, 2011).
[17]Lucas Kello, The Virtual Weapon and International Order (New Haven: Yale University Press, 2017).
[18]"Indian Government Websites Hacked by Pakistan Cyber Army," BBC News, December 2010.
[19] Ibid.
[20]Thomas Rid, Cyber War Will Not Take Place (London: Hurst, 2013).
[21]"India-Pakistan Cyber Tensions Rise," The Diplomat, October 2015.
[22]Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," Journal of Strategic Studies 38, no. 1–2 (2015): 4–37.

way blaming dynamic represents what researchers refer to as a cyber security dilemma, in which retaliatory actions of one state are viewed by the other as cyber assaults.[23]

So, although cyber tensions were most pronounced at this time, evidence suggests that it was a combination of hacktivism, suspicious intelligence activities, and political-related cyber disruptions and not necessarily the state-level cyberwarfare.

20172020: Critical Infrastructure Concerns and Defensive Shift: Since 2017, the world started to focus on critical infrastructure vulnerability. Cyberattacks of power grids and financial institutions at the international level created awareness of the strategic dangers of digital warfare.[24]

The situation in Pakistan, large-scale outages throughout the country happened in 2018 and 2021. Nevertheless, the official investigations explained such cases as technical failures and not as the proven foreign cyberattacks. This difference is significant to academic accuracy.[25]

In this stage, Pakistan was laying more emphasis on defensive cybersecurity. Cybercrime was regulated through the adoption of the Prevention of Electronic Crimes Act (PECA) 2016 allowing legal procedures to regulate cybercrime in Pakistan. Subsequently, in 2021, the National Cyber Security Policy was introduced as an attempt to strengthen the institutional capacity, critical infrastructure protection, and resilience to the cyber threat.[26]

Instead of the obvious sign of destructive outbound cyberwarfare, institutionalization of cybersecurity governance in Pakistan was more visible in the course of this time.

20212023: Regional Cyber Dynamics Emerging Threats: Between 2021 and 2023, the world experienced the growth of Advanced Persistent Threats (APTs), ransomware attacks, and the vulnerability of supply chains. One of the cybersecurity companies worldwide reported that there was heightened South Asian network targeting by multiple threat actors, some of which were purportedly state-related.[27]

In Pakistan, governmental agencies recognized the increased phishing efforts and data breaches of governmental institutions.[28] Nevertheless, these examples indicate that Pakistan is both a possible victim and player in regional cyber rivalry.

Regional cyber norms were also affected by diplomatic consultations in the United Nations Group of Governmental Experts (UN GGE) and Open-Ended Working Group (OEWG), where

[23] Buchanan, The Cybersecurity Dilemma
[24]Kim Zetter, Countdown to Zero Day (New York: Crown, 2014).
[25]Government of Pakistan, Ministry of Energy, “Report on National Power Outage,” 2021.
[26]Government of Pakistan, Prevention of Electronic Crimes Act, 2016.
[27]Government of Pakistan, National Cyber Security Policy, 2021.
[28]FireEye Mandiant, APT Trends in South Asia Report, 2022.
Pakistan Telecommunication Authority (PTA), Annual Report 2022.

Pakistan has actually been in favor of multilateral means of cyber governance in addition to national defense capability.[29]

Therefore, the 20212023 phase represents a more developed cybersecurity disposition of resilience, sharing of threat intelligence and law frameworks, as opposed to visible cyber aggression.

Attribution and the Complex of State Responsibility: It is also difficult in nature to categorize cyberattacks as a state. The non-state actors, patriotic hacker groups, intelligence services, and criminal organizations are often involved in cyber operations as they operate within the same networks.[30]

In Pakistan, the publicly available evidence does not confirm the direct authorization of major destructive cyberattacks by the state in 2010-2023 unconditionally. Rather, the trend indicates:

- Hacktivist competitiveness is associated with India- Pakistan tensions.
- Accusatory diplomatic histories.
- Increasing defensive cybersecurity institutionalization.
- The involvement in international cyber norm talks.

This delicate approach does not make any exaggerations and corresponds to the contemporary scholarly work on cyber conflict in South Asia.

Part 3

Defense Strategies: In this chapter, the author examines cyber defense measures that have been adopted by Pakistan against various threats. The author is trying to revisit the models of legislations, technology developments, and international collaboration, to assess the type of threats that Pakistan is confronted with and the defensive mechanisms it has established against it. Now more than ever, with the digital infrastructure, there is a need to suspect that the security of the digital infrastructure is of paramount concern to the national security and the economic stability. Pakistan like other states has a chronic cyber security problem whether it is the state or non-state actors and it necessitates the use of a sound defense mechanism. This heading lingers on the cybersecurity posture of Pakistan that is concerned with the cybersecurity rules, projects and partnerships aimed at eradicating the cyber vulnerabilities and developing resilience.

Policy Frameworks:

- National Cyber Security Policy: National Cyber Security Policy, that was sold in 2014 by author to interrogate it on all angles. The policy also provides the commitment of

[29] United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021.
[30] Thomas Rid, Cyber War Will Not Take Place.

the government to the development of cybersecurity in not only the governmental sector, but also in the financial, energy and telecommunication critical sectors. Major tasks will be listed as the reinforcement of law and regulations, the enhancement of emergency response, and the establishment of both the private and the governmental alliances.

- The Legislation and Regulatory Measures: The article also examines the actions of laws and controls which contribute to the increased security of cybersecurity in Pakistan. The promulgation of Prevention of Electronic Crimes Act (PECA) in 2016 stipulates the existence of multiple legal tools of combating cybercrimes, and cyber-bullying, child abuse, and government web hacking. In addition, the articles which must relate to the creation of data protection laws, encryption standards, and cybersecurity standards will also be mentioned here.

Technological Advancements:

- Indigenous Cybersecurity Solutions: The author will survey Pakistan on its effort to develop effective cybersecurity solutions to the country to ensure that it can effectively resolve its security concerns. Some of these efforts are investigated such as opening cybersecurity research institutes, cyber incubation centers, innovation center etc. The writer evaluates the effectiveness of such innovative programs in providing an enabling environment on innovation, which strengthens the competitiveness and dynamism of future cyber defense technologies.
- Cybersecurity Awareness and Capacity Building: The second section is on the programs of the government regarding the promotion of cyber security by creating awareness and skills to the stakeholders. To the authors, cybersecurity education and training programs are viewed as examples, which are essential to governmental officials and employees, law enforcement agencies, academic institutions, and the private sector specifically. The role played by public hosted events i.e. cybersecurity workshops and seminars in establishing the climate of cybersecurity practice is explored.

International Collaboration:

- Bilateral and Multilateral Partnerships: The author examines the relationship of Pakistan with foreign organizations, cyber companies with experience, and foreign governments.to develop its cyber defenses somewhat more robust. In this regard, emphasis is put on bilateral cooperation arrangements, information sharing systems, and combined planning of exercises. The author indicates that joint work has advantages in terms of the threats posed by cyberattacks, the establishment of interoperability, and the establishment of trust and confidence in cyberspace.
- Regional and Global Initiatives: This section examines how Pakistan takes different strides in the regional and global endeavors to idealize the cybersecurity cooperation. The author points out how the congregation of Pakistan has been

congregated in several global meetings such as the Shanghai Cooperation Organization (SCO), the South Asian Association of Regional Cooperation (SAARC), and the United Nations Group of Governmental Experts (UN GGE) on cyberspace. The influences of the regional mode of thinking and agreements on the policy adoption that would promote law-abiding behavior in cyberspace is also addressed.

The defense measures against cyber hazards used by Pakistan include a conglomeration of activities that is aimed at enhancing the cyber security, development of new techniques, and promotion of international collaboration. To illustrate, the policy frameworks such as the National Cyber security policy chart the route towards improved management of cyber risks similarly, the legislative and regulatory tools deployed in the implementation of the law are utilized in the prevention and prosecution of cybercrimes. To start with, the advancement of technologies demands the urgency in cyber security, and the subsequent international cooperation and awareness campaigns would assist Pakistan in acquiring the cyber defense level across the whole digital environment.

Conclusion:

The paper will offer an in-depth analysis of Pakistan's participation in the cyber warfare, both in terms of the supposed state-sponsored activities and the development of protection policies. The results show that the cyber posture in Pakistan is indicative of the regional processes, institutional evolution, and strategy. Since digital technologies have turned into the core of state authority, the nation has been striving to improve its ability to exercise influence and protect the vital networks. The review indicates the technical nature of cyber operations, in which the matters of attribution, technical advancement, and the geopolitical setting meet.

The cyber strategy of Pakistan demonstrates a multidimensional approach. It integrates legislative tools, policy frameworks, institutional mechanisms, and technological initiatives in order to respond to emerging threats. The legal, administrative, and operational measures are based on the National Cyber Security Policy 2021 and the Prevention of Electronic Crimes Act (PECA) 2016, which are the national frameworks. The institutional actors, such as the PKCERT and NCCIA, are involved in the response to incidents, threat intelligence, and capacity building. Policy, technology, and institutional coordination are aimed at helping Pakistan reduce vulnerability and increase resilience against the recurring cyber threats.

The interaction between the geopolitics of the region and cyber strategy is also highlighted in the research. The issue of the digital security of Pakistan is connected with the strategic rivalry, regional conflicts, and international relations. The role of cyber threats in this case is more than an issue of technical difficulty, but it is associated with a larger view of national sovereignty, political signaling, and strategic deterrence. As the paper demonstrates, the development of the cyber posture in Pakistan is both influenced by the internal factors,

including building capacity, law reformation, and enactment of policies, and external factors, such as regional rivalry and international cybersecurity standards.

Besides, the paper identifies the current drawbacks that come with the building of national cyber capabilities. The lack of technical expertise, the availability of resources, policy enforcement gaps, and the technological change at a rapid pace are constant threats. The new technologies, such as artificial intelligence, machine learning, and more sophisticated malware, demand dynamic governance and continuous policy-making. It is proposed in the literature that regular training, awareness campaigns at the national level, and collaboration with other countries are crucial in ensuring that cybersecurity practices remain effective.

The research can help in the understanding of cyber conflict in South Asia because it incorporates the theoretical perspectives of realism, constructivism, and institutional analysis. It shows the contribution made by the strategic goals, the way threats are perceived, and the institutional capacity to define the cyber posture of a state. It further highlights the criticality of the subtle analysis that is evidence-based when evaluating the efficacy and issues of national cyber approaches.

The implications are important to policymakers and practitioners. A solid knowledge of the cyber activities, weaknesses of the security meat, and the strategy used in defense within Pakistan can shape the policy-making, boost collaboration on cybersecurity in the region, and shape investments in cybersecurity infrastructure. The paper highlights that cyber defense cannot be just a technical activity but a multidimensional policy issue, which has to be coordinated at the government, industry, and civil levels.

Overall, the experience of cyber warfare in Pakistan shows that a multi-faceted, adaptable, and combined approach is necessary to protect the digital infrastructure in the country. Legislature integration, institutional capacity, technological advancement, and international collaboration have created a case study for other developing countries that are facing the same predicament. Following the ever-changing nature of cyber threats, governance, capacity building, and strategic planning will be of significant value over the long-term in ensuring that digital ecosystems are resilient, safe, and can sustain national and regional stability.

Bibliography:

Ahmad, Sara. "Cyber Security Threat and Pakistan's Preparedness: An Analysis of National Cyber Security Policy 2021." Pakistan Journal of Humanities and Social Sciences Research 5, no. 1 (2022).

Buchanan, Ben. The Cybersecurity Dilemma. Oxford: Oxford University Press, 2017.

FireEye Mandiant. APT Trends in South Asia Report. 2022.

Government of Pakistan. National Cyber Security Policy 2021. Islamabad: Ministry of Information Technology & Telecommunication, 2021.

Government of Pakistan. Ministry of Energy. "Report on National Power Outage." 2021.

Government of Pakistan. Prevention of Electronic Crimes Act (PECA). 2016.

Kello, Lucas. The Virtual Weapon and International Order. New Haven: Yale University Press, 2017.

Masood, Salman. "Pakistan Power Outage Plunges Country Into Darkness." The New York Times, January 9, 2021.

Naseeb, Jannat. "Framing the Digital Threat: Cybersecurity and Strategic Narratives in India-Pakistan Relations." International Journal for Conventional and Non-Conventional Warfare (2025).

Patil, Sameer, and Anirudh Kanisetti. "Cybersecurity in South Asia." Observer Research Foundation, 2019.

Pakistan Telecommunication Authority (PTA). Annual Report 2022.

Rid, Thomas. Cyber War Will Not Take Place. London: Hurst, 2013.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." Journal of Strategic Studies 38, no. 1–2 (2015): 4–37.

Shabbir, N., et al. "Cyber Security: A Growing Challenge to Pakistan." 2025.

"The India-Pakistan Cyber Tensions Rise." The Diplomat, October 2015.

"Indian Government Websites Hacked by Pakistan Cyber Army." BBC News, December 2010.

"Indian Government Websites Hacked by Pakistani Group." The Times of India, December 2012.

"Pakistan Cyber Army Claims Attack on Indian Websites." BBC News, September 2016.

United Nations. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2021.

Zetter, Kim. Countdown to Zero Day. New York: Crown, 2014.