Wah Academia Journal of Social Sciences
Volume 4, Issue 1, Jun 2025, pp. 1101-1119
ISSN – E 2958-8731 P 2958-8723

Caught in The Crossfire: Pakistan Cyber Security Dilemma in the India – China Cyberwar (Post Galwan Valley Clash)

Ameer Hamza[1]

Abstract

This study analyzes Pakistan cybersecurity dilemma in the context of escalating India – China cyberwar following the Galwan Valley Clash in June 2020. This study also explores how Pakistan balances its complex geopolitical position between two cyber giants by using classical realism as the theoretical framework, particularly emphasize on the work of Hans Morgenthau and Keneth Waltz. This study uses a qualitative methodology that includes document analysis and case study analysis, focusing on cyber incidents that occurred from February 2020 to May 2025. The findings of the study indicate that Pakistan faces significance challenges due to its geographical location, technological dependencies and limited cybersecurity capabilities. The research shows how Pakistan cybersecurity posture reflects broader realist assumptions of strategic hedging and power balancing. Key findings include Pakistan vulnerability to collateral damage from India – China cyber activities, Pakistan strategic reliance on Chinese cybersecurity technologies, and the security dilemma created by its dual relationship with both regional powers. The conclusion of this study is that other middle powers who deal with the same challenges can learn a lot from Pakistan experience as it provides a valuable insight. This research provides solutions based on realist principles includes indigenous capacity building, strategic diversification of cybersecurity partnerships, and the development of a defensive cyber doctrine. This approach helps to understand how technological interdependence creates new vulnerabilities while traditional security issues still exist in the digital age.

Keywords: Pakistan cybersecurity, India – China cyberwarfare, Galwan Valley Clash, Realism theory, Great Power Competition, Middle Power Dilemma, Strategic Hedging, Cyber Domain, South Asian Security, Geopolitical Positioning

[1] Department of International Relations, University of Management and Technology (UMT), Lahore – Pakistan

Introduction

The territorial clash between India and China over the territory of Aksai Chin stretch back across the last century. After the long month Sino – Indian War of 1962 China claiming Aksai Chin but the region has remained a flash point (Singh, 2020). Since the war, Indian and Chinese troops have patrolled the border, clashing occasionally in small skirmishes that have had far reaching implications for regional security dynamics.

Once again, things escalated in the summer of 2020. The India – China relationship has become increasingly complex and challenging with bilateral tensions rising to their highest point in decades following the Galwan Valley Clash (Joshi, 2021), sent shockwaves through both countries as it marked the first time since 1975 that soldiers were killed in combat along the border. Whereas India wanted to catch up the infrastructure developments of China, and India also had been improving infrastructure near Line of Actual Control (LAC), including building the Darbuck – Shyok – Daulat Beg Oldi (DSDBO) road, which is critical for accessing northern Ladakh (Shukla, 2020). China viewed this as a strategic threat because LAC is not clearly demarcated.

In early June 2020, both sides agreed to disengage. However, Indian soldiers went to verify Chinese withdrawal in the Galwan Valley, but a violent hand – to – hand clash broke out, leading to deaths on both sides. Twenty Indian soldiers lost their lives (Reuters, 2020). This was the fiercest border conflict with China to have occurred after the 1962 war. Today, tensions have calmed somewhat, with both sides agreeing to mutual withdrawals along parts of the border and engaging talks to end the standoff, an undercurrent of hostility has remained. Indeed, one significant achievement of the Galwan Valley clash has been a surge in cyber war between these two giants. These attacks have targeted a wide range of Indian government and corporate networks, and has caused significant damage. Though Beijing has denied any involvement in these attacks, cyber security companies like Recorded Future and CyFirma have reported cyber espionage activity by Chinese state – linked hacker groups targeting Indian assets and infrastructure (Recorded Future, 2021 & CyFirma, 2020), particularly affecting Pakistan strategic positioning and cybersecurity environment, it faces unique challenges and demands careful analysis through the lens of realism because geographic and geopolitical location between these two cyberwarfare opponents.

For Pakistan, which has complex relations with both countries - a strategic partnership with China and hostile relations with India - Pakistan faces a complex dilemma as a result of this cyberwarfare that affects its economic interests, diplomatic flexibility, and national security (Ahmad, 2021). Pakistan cybersecurity challenges are further exacerbated by its limited national cybersecurity skills, strategic dependencies, and relatively new digital infrastructure make it vulnerable to direct attacks and collateral damage from India - China cyber operations.

Theoretical Framework

In order to understand Pakistan cybersecurity behavior in the context of India - China cyberwar, this study uses classical realism as its primary theoretical framework, specifically referencing the work of Hans Morgenthau and Kenneth Waltz (Morgenthau, 1948 & Waltz, 1979). The basic principles of Realism regarding power dynamics, state behavior, and security dilemmas offer substantial insight into Pakistan strategic responses to cyber threats.

- **Core Realist Assumptions**

According to classical realism, states are the primary actors in international relations and operates in anarchy, with no supranational body able to ensure security (Waltz, 1979). With few international governance structures and unclear norms controlling state behavior, this anarchy is even more evident in the cyber domain. This means cybersecurity is essentially a self-help activity for Pakistan, requiring independent capacity building and strategic decision making.

Understanding cybersecurity dynamics is especially relevant to the realist emphasis on power as the primary currency of international relations (Morgenthau, 1948). Cyber capabilities are a new kind of power that can be used to gather intelligence, achieve political goals, and cause economic harm. Pakistan limited cyber power in comparison to China and India creates vulnerabilities that need to be managed through defensive capabilities, strategic alignment, and diplomatic maneuvering.

- **Security Dilemma in Cyber Domain**

A fundamental concept in realist theory, the security dilemma, appears specifically in cybersecurity (Herz, 1950). India and China viewed Pakistan efforts to strengthen its cyber defenses as offensive capabilities, which could lead to retaliatory actions

that eventually weaken regional security. This dilemma is particularly given Pakistan hostile ties with India and strategic partnership with China.

Additional security problem dynamics are created by Pakistan technology collaboration and CPEC integration into Chinese cybersecurity ecosystems. Chinese technology gives Pakistan the skills it lacks, but it also creates dependencies and vulnerabilities that India may take advantage of. In the same way, cybersecurity risks associated with Pakistan use of Indian IT services and software must be measured against financial gains.

Methodology

In order to understand Pakistan cybersecurity dilemma in the India – China cyberwar, this study uses a qualitative method which include document analysis, case study examination, and theory application (Creswell, 2018). In order to create a detailed picture of Pakistan strategic challenges and responses, the study focusses on a variety of information sources and use realist theory as its analytical framework.

- **Data collection**

Primary sources of data collection are official government documents, cybersecurity plans, diplomatic declarations, and parliamentary proceedings related to Pakistan cybersecurity policy. Incorporates Pakistan National Cybersecurity Policy (2021) and statements from officials like Former Ex-Prime Minister of Pakistan Imran Khan and Pakistan Telecommunication Authority (PTA) (Government of Pakistan, 2021).

Secondary sources are media analysis, cybersecurity industry reports from organizations like Recorder Future and CyFirma and expert interviews that offers contextual understanding of regional cybersecurity dynamics. The core focus of this research is how Pakistan is impacted by the escalation between India and China after Galwan Valley clash (June 2020 to present).

- **Analysis and Findings**

From a realist point of view, the India - China cyberwarfare had a significant impact on Pakistan cybersecurity, emphasizing the anarchic structure of the international system in which Pakistan is protecting its national interests with navigating great power competition.

The cyberattack timeline and Security implications

February 2020: The world was in the early stages of COVID – 19 Pandemic, government agencies, healthcare organizations, medical research institutions and hospitals in Wuhan, China and other cities dealing with the Pandemic are targeted because they are involved in the critical research, epidemiological data, and healthcare operations. Indian State backed hackers would deploy phishing emails that appear to be from reputable health organization (e.g: WHO, Chinese health ministries, or global health bodies) to extract critical research data (FireEye, 2020). From a realist point of view, this highlights how government uses cyber operations to advance their national interests during times of crisis.

May 2020: Chinese hackers started attacking important Indian industries such as financial institutions, telecommunication, and defense. Attack on government websites and digital infrastructure were noted in reports (CheckPoint Research, 2020). This escalation reflects realist idea of power projection and strategic competition, as both sides try to obtain relatives gains through cyber operations.
June 2020: A study conducted by US bases cybersecurity company Recorded Future, specializing in threat detection and analysis, shows that Chinese malware has infected Indian power control systems. They targeting India technology and banking facilities across five days. They enact over 40,000 hacking attempts, combination of DDoS and Phishing attempts. The Chinese hackers attempting to access sensitive data of Indian military and strategic intelligence (Recorded Future, 2021). In response India retaliated by banning Chinese apps like TikTok and WeChat (Reuters, 2020). Being caught between these enemies, Pakistan saw repercussions as its network were targeted as collateral. Indian retaliatory ban on Chinese apps showed how cyberwarfare crosses technological boundaries and becomes an economic struggle.

October 2020: Mumbai, India's business hub faced a several blackouts on October 12, 2020. Recorded Future emphasized that this was a result of multiple malwares deployed by Chinese group RedEcho (Recorded Future, 2021). Serves as an example of how cyberwarfare can achieve strategic goals without using conventional military force. For Pakistan this incident highlighted the potential for ripple effects across interconnected systems and vulnerabilities in the regional power grid.

August 2023: Ahead of and during the G20 Summit in New Delhi, Indian cybersecurity agencies had reported 1.6 million hacking attempts per minute. China, Myanmar, Cambodia, and Dubai are traced through IP analysis using Chinese – controlled botnets (Indian Computer Emergency Response Team, 2023). They are using the same tactics as used in previous Pakistani hacktivist groups which shows the possibility of both China and Pakistan behind these cyber-attacks and blurring traditional alliance boundaries.

October 2023: Team Insane PK, a Pakistan based hacking group launched a coordinated cyber campaign, #OpIndia They executed over 2,450 attacks on Indian server and leaked 100GB sensitive data by using Chinese APTs, APT41, and Mustang Panda. Indian cybersecurity believes Chinese actors enabled the execution by providing technical support (CyFirma, 2023). This partnership highlights how Chinese capabilities influenced Pakistan cybersecurity posture, reflecting realist ideas of forming alliance to maximize security.

May 2025: Pakistan with the help of Chinese coordination launched a cyberattack on internal networks of two of India's top defense related institutions. Publicly attributed to Pakistani hackers but the malware used had code similarities with Chinese state sponsored APTs like RedEcho and Naikon (Threat Intelligence Report, 2025). This recent development highlights Pakistan's growing involvement in Chinese cyber operations while preserving credible denial.

Realist Analysis of Security Impacts

The escalation highlights classical realist dynamics in which Pakistan is faced with a security dilemma: collaboration with China enhances cybersecurity capabilities but also makes Pakistan more vulnerable to Indian repercussions. In the struggle between India and China, Pakistan cybersecurity infrastructure has taken on a secondary role as both countries aim to get continuous access to Pakistani systems for intelligence collection and possible future operations.

According to the "Cybersecurity in Pakistan" report by the Pakistan Telecommunication Authority (PTA), cyberattacks on government websites and important infrastructure have increased noticeably in recent years, most likely as a result of the ongoing rivalry between China and India (Pakistan Telecommunication Authority, 2022). Former Pakistani Prime Minister Imran Khan mentioned India

cyberattacks and military presence close to the border as a security threat for Pakistan and preparing for cyberattacks, particularly considering it strategic significance in South Asia, reflecting realist concerns over national security (Khan, 2021).

Pakistan cybersecurity posture is a reflection of larger realist calculation between China and India on geopolitical positioning, power and security. The country's strategy highlights its efforts to maintain flexibility in relationship with both regional powers to maximize security.

Strategic Hedging and Cyber Alignment

Pakistan as a neighbor state has indirect threats from the cyber conflict between China and India because they are engaged in a longstanding strategic rivalry, often clashing on territory and then engaged in cyber operations. As Pakistan uses cyber defense strategy to enhance its strategic position in the region, its cyber security capabilities influence its relation with both India and China, it is natural that Pakistan is sitting between them and become a victim or involved in this cyber struggle. For example, cyberattacks were launched during the 2019 India – Pakistan crisis. Hacking groups from India and Pakistan attacked on each other official websites (Kaspersky, 2019). Cyberattacks can increase as a result of the regional crisis. This shows the realist viewpoint that security is the primary concern of a state and the presence of external threat often drives a nation to strengthen its own defense capabilities.

Pakistan is historically allied with China and it could strengthen its cyber defense capabilities by joint cyber defense initiatives, emphasizing Realist view that nation's military and economic posture shapes its geopolitical alliances and posture (Mearsheimer, 2001). Realists suggest that states align themselves with others that provide security benefits. Pakistan relation with China and India directly impacted by its cyber security posture. Pakistan may be more at risk of outside pressure or attacks if it is seen as weak in this area which could lead to strong relation with China or Russia.

According to the National Cyber Security Policy of Pakistan (2021), as a part of its Security Policy, Pakistan is focusing on its cyber defense system in response to the threats posed by India and evolving nature of the global cyber threats (Government

of Pakistan, 2021). Prime Minister Imran Khan statement reflects Pakistan Realist strategy of enhancing self-defense capabilities and realists concerns over national security.

Alliance Dynamics and Power Balancing

Beyond simple bilateral ties, Pakistan cybersecurity alliances highlight complex alliance dynamics. Pakistan efforts to develop domestic capabilities while preserving strategic alliances are shown by the creation of organizations such as the National Response Centre for Cyber Crimes (NR3C) under the Federal Investigation Agency's (FIA) (National Response Centre for Cyber Crimes, 2020).

However, Pakistan's cyber security posture in comparison with India could decide its security posture in future conflicts. With a strong defense system. Pakistan may become more powerful in its geopolitical positioning and less vulnerable to cyberattacks with a strong defense system, emphasized realist's expectations about how capabilities influence strategic partnership.

According to realist theory, a state's technological and military capabilities play a important role in its ability to survive in a competitive and anarchic international system. Pakistan's technological capacity in the cyber domain is critical to its survival and ability to counter the ripple effects of any cyber escalation between India and China.

Capability Assessment through Realist Lens

Although Pakistan's technological capacity to face a cyber conflict is limited compared to China and India, both of which invest heavily in cyber warfare and defense systems. According to a 2019 report by the Global Cybersecurity Index, Pakistan ranked 74th globally in terms of cyber security preparedness, indicating room for improvement. This is a stark contrast to China, which is ranked 1st, and India, ranked 47th (International Telecommunication Union, 2020).

However, Pakistan has made notable advancements in its cyber capabilities like the National Response Centre for Cyber Crimes (NR3C) under the FIA (Federal Investigation Agency) to tackle the growing threats in the digital space. Realist

theory would suggest that these measures are part of Pakistan's broader strategy to safeguard its sovereignty and mitigate the effects of any cyber escalation.

Despite these efforts, Pakistan's cyber infrastructure is still relatively underdeveloped compared to regional powers like India and China. Vulnerabilities in its civilian and military networks remain, as evidenced by repeated cyber-attacks over the years. Dr. Ismail Shah, former Chairman of PTA, has noted the critical need for Pakistan to modernize its cyber security framework to better defend against increasing threats, including those stemming from regional tensions (Shah, 2021).

Security Dilemma in Technological Development

When it comes to cybersecurity development, Pakistan faces a fundamental security dilemma, as depending on foreign technology creates dependencies that enemies might take advantage of, while developing its own capabilities costs resources that could otherwise reinforce conventional defenses. Given Pakistan financial limitations and conflicting development agendas, this dilemma is especially serious. According to the realist perspective, Pakistan technological limitations limit its strategic opportunities and make it more vulnerable to manipulation by superpowers. Pakistan is forced to pick between Chinese and Indian technologies due to its limited domestic cybersecurity capabilities while each has unique security concerns and alliance duties.

Discussion and Implications

According to the analysis, Pakistan cybersecurity dilemma is representative of larger trends in middle power conduct during great power struggle. In anarchic international system, Pakistan answers show logical attempts to maintain strategic flexibility while maximizing security. With Pakistan experience acting as a case study for how smaller countries handle the difficulties presented by Great power rivalry in the cyber space, the findings show how cybersecurity has become deeply connected to traditional geopolitical processes.

- **Strategic Constraints and Realist Explanation**

In numerous of significant aspects, Pakistan cybersecurity policies are consistent with fundamental realist assumptions on state conduct, Realistic view of power disparities and the necessity of avoiding total reliance on either China or India are

reflected in the nation balancing strategy (Waltz, 1987). Pakistan has demonstrated an awareness of resource limitations and the potential for escalation with more powerful neighbors by emphasizing defensive capabilities above aggressive cyber activities.

Realist principles of flexibility and avoiding getting caught up in large power struggles are reflected in Pakistan cybersecurity policy. Pakistan maintains its flexibility in responding to shifting conditions by declining to specifically name the main cyberthreats or take sides in the Indian - China cyberwar. This strategy is most prominent in Pakistan diplomatic remarks about cyberattacks, as representatives always stress the broad guidelines of cybersecurity collaboration while avoiding accountability.

Pakistan actions show how state strategies are shaped by the distribution of cyber capabilities from a structural realist point of view (Waltz, 1979). Pakistan policy options are limited by structural factors resulting from the imbalance between its inadequate national cyber capabilities and advanced offensive capabilities of China and India. These limitations are evident in Pakistan careful balancing of public statements on regional cyber conflicts, its reliance on defensive alliances, and its hesitation to develop exclusively offensive cyber weapons.

Compared to large powers, Pakistan faces a particular cybersecurity dilemma. Pakistan limited resources require more challenging trade - offs, whereas China and India can pursue cyber capabilities that improve both defensive and offensive postures. Other security objectives have to be sacrificed in order to invest in cyber defense capabilities, resulting in opportunity costs that are not as great for larger powers. This dynamic limits Pakistan strategic autonomy while strengthening its reliance on outside alliances.

- **Regional Security Implications**

The cybersecurity issues facing Pakistan have greater consequences for the security and stability of the South Asian region. Through cyber domain interactions, the nation's vulnerabilities raise the possibility of an escalation between China and India, while its strategic responses affect the region overall power dynamics. Because regional cyber infrastructure is interconnected, attacks that target one nation frequently affect its neighbors, posing a risk that extends beyond bilateral ties.

With careful hedging and diplomatic management, middle powers can preserve some strategic autonomy on cybersecurity issues, according to Pakistan experience. The secret is to develop enough domestic skills to preserve policy flexibility without being totally dependent on any one partner. However, structural challenges that are difficult to address with policy changes alone, such as geographic vulnerabilities, lack of resources, and technical dependence, limit this autonomy.

Beyond South Asia, the regional implications reflect on more general trends in global cybersecurity policy. The situation in Pakistan highlights how smaller nations trapped between rival cyber giants have unique difficulties due to the lack of strong international cyber standards and institutions. Pakistan is forced to explore bilateral agreements that would undermine its strategic flexibility in other area due to its inability to rely on international law or multilateral institution for cyber protection. Moreover, India may be able to take advantage of the new dependencies that Pakistan cybersecurity alliances with China have produced. While Pakistan increasing coordination with Chinese cyber actors raises the possibility of Indian retaliation the integration of Chinese technology into Pakistan critical infrastructure creates weaknesses that Indian cyber operations might target. This interplay highlights how, depending on the larger geopolitical background, cybersecurity collaboration can both strengthen and weaken national security.

- **Proposed Solutions Based on Realist Framework**

This section offers practical solutions based on fundamental realist ideas of power maximization, security enhancement, and strategic autonomy preservation, drawing on the realism analysis of Pakistan cybersecurity dilemma in the India - China cyber war. These solutions identify ways to strengthen Pakistan cybersecurity stance within the anarchic international system while acknowledging the structural limitations it faces.

- **Indigenous Capacity Building Strategy**

Realist theory emphasizes self - help, the fundamental principle of state survival in an anarchic world (Waltz, 1979). To strengthen its strategic independence and reduce its dependence on outside forces, Pakistan must give top priority to building up its own cybersecurity capabilities. This requires an all-encompassing strategy that includes institutional strengthening, technology innovation, and human capital development.

As a specialized school focused to developing cybersecurity experts, researchers, and analysts, Pakistan ought to establish a National Cybersecurity University. This institution would accomplish several practical goals, including less dependence on outside knowledge, building up domestic knowledge bases, and producing human capital that may understand Pakistan specialized security landscape. To ensure through coverage of Pakistan cybersecurity demands, the university should provide programs ranging from technical cybersecurity capabilities to cyber policy and strategy.

Another essential element of capacity building is the creation of domestic cybersecurity research and development facilities. These centres need to focus on creating cybersecurity solutions that are unique to Pakistan, such as threat detection systems that are adapted to local infrastructure, incident response procedures that are modified to fit the institutional contexts of Pakistan, and defensive technologies that can function without assistance from external sources. From a realist perspective, such domestic capabilities increase Pakistan influence while reducing vulnerabilities to external influence.

Like military reserve system, Pakistan should establish a National Cyber Reserve Corps made up of cybersecurity experts from the government, business, and academia who can be called upon in the event of a cyberattack. This strategy reflects realist ideas of resource optimization in the pesuit of security objectives by optimizing existing human resources while preserving cost effectiveness.

- **Strategic Diversification of Cybersecurity Partnerships**

According to realist theory, in order to preserve strategic flexibility and reduce vulnerability to pressure or withdrawal, nations should avoid from excessive dependence on single ally (Mearsheimer, 2001). Pakistan current heavy reliance on Chinese cybersecurity technology and expertise creates vulnerabilities that India could take advantage of while limiting Pakistan strategic options in future crisis.
Cooperation with European Union nations, especially those with significant cybersecurity capabilities but few geopolitical disputes with Pakistan, could be an element of Pakistan multi-vector cybersecurity partnerships strategy. Without the strategic complexities of big power partnerships, nations like Sweden, Switzerland, and the Netherlands provide advanced cybersecurity technologies and experience. This collaboration will reduce Pakistan dependence on China while giving it access to other cybersecurity resources.

Another way to achieve strategic diversity is to engage with middle powers that have comparable cybersecurity issues. Pakistan can look into collaborating on cybersecurity with nations like Brazil, South Korea, and Turkey, who deal with similar issues in managing cybersecurity while preserving great power strategic autonomy. These collaborations might include exchanging best practices, sharing technology, and coordinating responses to frequent cyberthreats.

Additionally, Pakistan should improve its cybersecurity connections with Gulf Cooperation Council nations, especially Saudi Arabia and the United Arab Emirates, which have made significant investments in cybersecurity capabilities and share Pakistan worries about regional stability. In line with Pakistan larger diplomatic goals, these collaborations may offer financial and technical resources for the advancement of cybersecurity.

- **Defensive Cyber Doctrine and Strategic Ambiguity**

Pakistan should create and publicly declare a defensive cyber doctrine that explains its cybersecurity objectives while preserving strategic uncertainty regarding particular capabilities and responses. Realist theory emphasizes the significance of precise strategic doctrine that maximize security while reducing the risks of escalation (Schelling, 1960).

The doctrine should highlight Pakistan dedication to defensive cybersecurity measures, such as protection of government system, civilian networks, and critical infrastructure. This defensive approach serves multiple realist objectives as it reduces the possibility of preemptive attacks by neighbors, establishes Pakistan as a responsible cyber actor in international forums, and allows Pakistan to develop cybersecurity capabilities without creating cybersecurity dilemma complications.
While avoiding offers that would reduce further flexibility, uncertainty regarding Pakistan unique cybersecurity capabilities and response processes will improve deterrence. While upholding its basic commitments to cybersecurity cooperation and responsible state behaviour in cyberspace, Pakistan should keep away from disclosing information about its response capabilities, attribution systems, or cybersecurity infrastructure.

The doctrine should also include that cybersecurity collaboration with China and India, as well as with all other regional partners, is subject to reciprocal respect for

Pakistan digital sovereignty. This strategy maximizes advantages while maintaining strategic autonomy, which reflects realist idea of conditional cooperation.

- **Economic Cyber Resilience Framework**

Realist analysis acknowledges the essential link national security and economic strength (Gilpin, 1981). Economic limitations that that limit investment in defensive capabilities and increase dependence on foreign technology and knowledge exacerbated Pakistan cybersecurity vulnerabilities. These economic factors must be taken into consideration for sustainable cybersecurity improvement.

Pakistan needs to establish a National Cybersecurity Development Fund that is funded by a mix of foreign development assistance, private sector donations, and government allocations. The formation of human capital, research and development, and cybersecurity infrastructure development would provide sustained funding from this fund. Long term sustainability and political independence should be ensured by fund structure, protecting cybersecurity investments from transitional political pressures.

Another essential element of economic resilience is the growth of domestic cybersecurity industries. Pakistan should offer tax benefits, research funding, and preferred government procurement practices as incentives for local companies to develop cybersecurity products and services. Such policies would provide financial incentives for private sector cybersecurity development and research while reducing dependence on foreign suppliers.

Pakistan should look towards exporting cybersecurity, especially to other developing nations dealing with same issues. Pakistan might increase its worldwide cybersecurity profile and generate revenue by becoming an expert in affordable, effective cybersecurity solutions that are suited to the needs of developing nations. Realist principles of converting defensive capabilities into sources of economic advantage and global influence are reflected in this strategy.

- **Institutional coordination and governance mechanism**

Realist theory emphasized the importance of strong state institution in managing security issues and carrying out strategic objectives (Krasner, 1978). Pakistan current cybersecurity institutional framework suffers from coordination issues, unclear

roles, and a lack of resources and fundings limit its effectiveness to combat complex cyberthreats.

At the highest level of government, Pakistan needs to establish a National Cybersecurity Council, led by the Prime Minister and officials from military, intelligence, telecommunication, finance, and from the field of foreign affairs. This council would provide collaboration among various government departments and agencies while offering strategic direction for Pakistan cybersecurity policies. The high-level composition of the council would provide enough political attention and funding for cybersecurity priorities.

The establishment of a unified National Cyber Command centre would centralize Pakistan cybersecurity response capabilities while maintaining coordination with existing institutions. This centre would act as the main focus for incident response, threat monitoring, and strategic planning without duplicating existing capabilities. The centre should have members from both military and civilian organizations.

Pakistan should establish official cybersecurity coordination channels with provincial governments. Recognizing that many critical infrastructure elements are under provincial jurisdiction. These channels should include frequent information sharing, coordinated response procedures, and joint training exercises to maintain national cybersecurity coherence while respecting federal structures.

Legal and regulatory structures require significant development to offer suitable foundations for cybersecurity initiatives. Pakistan should update its cybercrime laws to address emerging threats while ensuring that legal structures support rather than hinder cybersecurity activities. This includes clarifying authorities for government cybersecurity agencies, establishing clear protocols for international cooperation, and providing legal protections for cybersecurity workers.

- **Regional Cyber Diplomacy and Confidence-Building Measures**

Although realist theory places a strong emphasis on rivalry and conflict, it also acknowledges that, cooperation can serve state objectives when properly structured (Keohane, 1984). Pakistan should consider selective cybersecurity collaboration with China and India by implementing steps to foster confidence that lower the possibility of unintentional escalation while maintaining strategic adaptability.

A South Asian Cyber Security Dialogue involving China, India, and other regional countries should be proposed by Pakistan. The dialogue would focus on technical cooperation, information sharing regarding shared risks, and the creations of regional cyber standards that benefit all participants. Such multilateral engagement will establish Pakistan as a responsible regional actor while providing Pakistan with opportunity to impact regional cybersecurity developments.

Conclusion

Pakistan Cybersecurity dilemma in the India – China cyberwar demonstrates the challenges faced by middle power in the great power rivalry in cyber space. Realism emphasized the Pakistan efforts to maintain strategic flexibility as a logical attempt to maximizing the security to survive in an anarchic world with limited governance institutions and security threats.

According to the analysis, Pakistan cybersecurity dilemma is because of structural elements like geographic vulnerabilities, technological dependence and resource limitation. As Pakistan geographically lies between these two giants and become a natural victim of the impacts and also have dependence on China for its defense and economic initiatives and for resources like some natural resources depend on India so this all cannot be easily addressed just through the policy changes. However, Pakistan has shown that it is capable of adapting by creating defensive capabilities, hedging strategies and international partnerships to deal with these challenges in a way that it is consistent with realist assumptions regarding middle power behavior. Pakistan experience offers valuable insights for other middle power countries who deals with the similar cybersecurity challenges in great power competition. The key lessons which Pakistan is learned from this dilemma and other middle power countries should learned from this experience of Pakistan includes importance of strategic diversification, development of national capabilities and diplomatic management of complex partnership relationships while maintaining strategic ambiguity to maintain flexibility.

From a realist point of view, Pakistan cybersecurity dilemma reflects larger trends in international relations in the digital age, where technological interdependence creates new type of vulnerabilities while traditional security issues continue to exist. It is important to understand these dynamics for developing effective policies that

enhance security while maintaining strategic autonomy in a world that is becoming more interconnected but anarchic.

References

Ahmad, S. (2021). Pakistan's strategic dilemma in China-India rivalry. Institute of Strategic Studies Islamabad.

Check Point Research. (2020). Cyber-attacks during COVID-19: Analysis of regional threats. Check Point Software Technologies.

Creswell, J. W. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage Publications.

CyFirma. (2020). Chinese cyber espionage activities targeting Indian infrastructure. CyFirma Intelligence Report.

CyFirma. (2023). Team Insane PK: Pakistan-China cyber collaboration analysis. CyFirma Threat Intelligence.

FireEye. (2020). COVID-19 themed cyber-attacks: Regional analysis. FireEye Intelligence Report.

Gilpin, R. (1981). War and change in world politics. Cambridge University Press.

Government of Pakistan. (2021). National cyber security policy 2021. Ministry of Information Technology and Telecommunication.

Herz, J. H. (1950). Idealist internationalism and the security dilemma. World Politics, 2(2), 157-180.

Indian Computer Emergency Response Team. (2023). G20 Summit cyber threat assessment. Ministry of Electronics and Information Technology.

International Telecommunication Union. (2020). Global cybersecurity index 2020. ITU Publications.

Joshi, S. (2021). Understanding the Galwan clash: India-China border tensions and regional implications. Strategic Analysis, 45(3), 234-251.

Kaspersky. (2019). Cyber warfare in South Asia: India-Pakistan digital conflict analysis. Kaspersky Lab.

Keohane, R. O. (1984). After hegemony: Cooperation and discord in the world political economy. Princeton University Press.

Khan, I. (2021, March 15). Pakistan's security challenges in the digital age (Speech). National Assembly of Pakistan.

Krasner, S. D. (1978). Defending the national interest: Raw materials investments and U.S. foreign policy. Princeton University Press.

Mearsheimer, J. J. (2001). The tragedy of great power politics. W. W. Norton & Company.

Morgenthau, H. J. (1948). Politics among nations: The struggle for power and peace. Alfred A. Knopf.

National Response Centre for Cyber Crimes. (2020). Annual cybersecurity report 2020. Federal Investigation Agency.

Pakistan Telecommunication Authority. (2022). Cybersecurity in Pakistan: Annual threat assessment. PTA Publications.

Recorded Future. (2021). Chinese cyber operations targeting Indian power sector. Recorded Future Intelligence Report.

Reuters. (2020, June 16). Twenty Indian soldiers killed in clash with Chinese troops. Reuters.

Schelling, T. C. (1960). The strategy of conflict. Harvard University Press.

Shah, I. (2021). Modernizing Pakistan's cybersecurity framework: Challenges and opportunities. Pakistan Telecommunication Review, 15(2), 45-62.

Shukla, A. (2020). India-China border infrastructure development and strategic implications. Strategic Affairs, 28(4), 112-128.

Singh, R. (2020). Aksai Chin dispute: Historical perspectives and contemporary challenges. Observer Research Foundation.

Threat Intelligence Report. (2025). Pakistan-China cyber coordination: Latest developments. Regional Cybersecurity Analysis.

Walt, S. M. (1987). The origins of alliances. Cornell University Press.

Waltz, K. N. (1979). Theory of international politics. Addison-Wesley Publishing Company.

Article Information:

Received	*8-Apr-2025*
Revised	30-May-2025
Accepted	11-Jun-2025
Published	15-Jun-2025

Declarations:

Author's Contribution:

- **Conceptualization, and intellectual revisions**
- **Data collection, interpretation, and drafting of manuscript**
- The author agrees to take responsibility for every facet of the work, making sure that any concerns about its integrity or veracity are thoroughly examined and addressed

- **Conflict of Interest**: NIL
- **Funding Sources**: NIL

Correspondence:

Ameer Hamza

hamza.umt@gmail.com