Social Sciences & Humanity Research Review
ISSN 3007-3170(O), ISSN :3007-3162(P)
Volume 3 issue 1,pp. 40-60
January-March 2025

Received: 01 January 2025 ,Accepted: 15 January 2025
DOI: https://doi.org/10.33282/jssr.vx2i4.03

US-China Cyber Security Warfare: Implications on Pakistan (2018-2024)

[1]Muhammad Usman Ghani

[1]Student of BS Political Science, Department of Political Science and International Relations, University of Management and Technology, Lahore.

F2021126011@umt.edu.pk

Abstract:

The United States-China cyber rivalry viewed as a new reality not only in terms of global security, but also with regard to the role that technological competition assumes in the world system, and which has critical importance in regard to countries like Pakistan. Geographically located in a strategic position, Pakistan is faced with two dilemmas: threats of cyberattacks directed at its national critical infrastructure facilities and hopes of growth in technological capabilities with the assistance of both superpowers. This perspective looks at these dynamics from the offensive and defensive realist respectively in order to provide context on the cybersecurity capacities and strategies available to Pakistan. Cyber warfare, particularly AI-driven applications such as ransomware and cyber-espionage are analyzed for their consequences on Pakistan's current security and future expectations of cyber incidents, particularly with respect to the Belt and Road Initiative and the China-Pakistan Economic Corridor (CPEC). The focus of this research emphasizes that Pakistan strives to maintain her strategic neutral status, pursued advancements in cybersecurity regulations, and developed local technology to assert its sovereignty and maximize the chances of progress. With the analysis of cyber policies, the focus of the study is on how national policies should help maintain security with changing cyber threats. The results will be useful in devising strategies in a diversity of areas required for such developing countries to deal with the global cyber competition of the digital era.

Introduction:

Cyberspace has been seen as the key sector for competition among various nations in the 21st century which in turn has changed the security and power relations in the world. The international arena has been turned into a domain in which states have started using cyber means for influence, espionage and conflict (Bashir, H., Zarish, W., & Malik, R.2024). There is no greater competition than the one between the United States of America and China, both technological superpowers, who are in a spiraling race to cyber supremacy. Unlike wars in the past where physical boundaries and material interests shaped strategic calculations, this one is different, it knows no boundaries and draws upon the use of advanced technologies including artificial intelligence (AI), cyber-warfare and sabotage of infrastructure to achieve suffice political, economic and military goals and resources (Arquilla, J. 2019). United States and China have a cyber competition which represents a more worrying trend of competition for world order in the current times where an emphasis on technology and information has become a focal point of power (Kello, L. 2018). United States, the historical leader in software, cloud computing and cybersecurity ecosystems, endeavors to preserve its position whenever it seeks to gain advantage in technology while influencing cyber order. While on the other hand China has rapidly advanced AI, 5G and other aspects of infrastructure and as such poses a serious challenge to the US (Nye, J. S. 2021).

Projects like the Digital Silk Road have enabled China to Increase its presence in Asia Africa and other regions by exporting digital technologies and positioning itself in the rising global digital economy. Such a rivalry has consequences that go beyond the borders of the countries involved, affecting the policies of other nations caught in between the digital arms race (Shahid, M. 2021). Cyberattacks, data leaks, AI-controlled espionage campaigns, as well as digital influence operations have increasingly become the order in the relations of states, thus endangering the sovereignty, stability and security of nations worldwide (Zhao, W. 2020). For smaller or less developed countries in terms of their cybersecurity centers like Pakistan, the risk is incredibly great.

This rivalry has serious consequence for Pakistan as a nation and its strategic worldview. Pakistan occupies a critical position both geographically and politically and can be termed as a contestant and an observer in the US-China cyberspace reality (Abbas, T. 2023). Due to the increasing dependence of Pakistan on mobilization of digital systems for its governance, economy and even national security especially given Pakistan’s key position in initiatives such as CPEC, it is highly exposed to the consequences of such rivalry (Khan, A. 2022). Such over-reliance on digital technology can make Pakistan vulnerable to several cyber-attacks, such as, cyber-espionage, ransomware, and critical infrastructure disruption. Consequently, geographical constraints imposed by both the US and China put Pakistan in areas of decision-making that would either strengthen Pakistan’s technological development or throw it into this technologically driven cyber war as a target (Khan, A. (2022). The effects of the United States-China rivalry on Pakistan are several. On the one hand, the competition enables Pakistan to attract investments from both countries in the form of technologically advanced tools and cybersecurity skills (Iqbal, S. 2020). Investments made by China into infrastructure and technology as channeled through the CPEC scheme stand to be beneficial for Pakistan’s goals of securing advanced cyber capabilities as well as developing modernization of information technologies within the country. Likewise, combined efforts with the United States would make it possible for Pakistan to acquire modern cybersecurity technologies and training, which in turn, significantly boost Pakistan’s readiness in psychologically sophisticated cyber warfare (Ahmed, H. 2024).

Pakistan is packed between its historical leftist tendencies and the new governmental framework that is heavily reliant on China as its ally. The footprints of these policies that seek class collectivization, redistribution, and deployment of all available material resources are apparent in the new government’s strategy (Khan, A. 2022). The contradictions that are created in a state that seeks supremacy in all forms such as political, ideological, and economic determines the behavior and implements policies that are detrimental to every cycle of government formation and consolidation ultimately defining the struggle that is synonymous with the history of Pakistan (Iqbal, S. (2020). Security instabilities however do not solely restrict the control to factions out of a power imbalance rather control is also drawn from micro politics that takes place to establish a caste system that sees the displacement of the weaker without replacing them with stronger and aiming for independence as a state, this reality is what has always perturbed the course of politics inside Pakistan (Ming, L. 2023). What is even more ironic is the amount of support that China has vowed to give to Pakistan in the form of economic funding however these never seem to turn into reality which only adds to the soft power shift and global order reconfiguration that is witnessed making Pakistan's attempts for geopolitical balance all the more convoluted in execution (Ahmed, H. (2024).

This research investigates the ramifications of the cyber warfare between the US and China on Pakistan, particularly in relation to its cybersecurity, its foreign alliances, and foreign policy formulation. The study attempts to find out the way Pakistan can address AI based cyber security challenges while optimizing the technological development in the country as well. Using a two-prong theory approach, Defensive Realism which explains Pakistan's security expenditures and Offensive Realism which explains the hegemonic behavior of the US and China, the paper seeks to explain why the global cyber strategies interface with Pakistan's interests (Khalid, R., & Ahmed, S. 2023). As an example, Defensive Realism, focuses on maintaining sovereignty and survival from external aggression, supports the understanding of why Pakistan requires adequate cyber security, a non-aligned geo-political stance, and strong investment in local technology. In contrast, Offensive Realism accounts for the US and China's aggressive cyber strategies, which add further threats to Pakistan's national security and independence. By combining these elements, this paper calls for developing and implementing more effective strategies for securing cyberspace and determining the right direction of national policies which are necessary for the sustainable development of Pakistan.

Research Questions:

1. How does the US-China cyber rivalry shape Pakistan's strategic alliances while impacting its cybersecurity infrastructure?
2. What strategies can Pakistan adopt to mitigate threats posed by AI-driven cyber warfare between the United States and China?

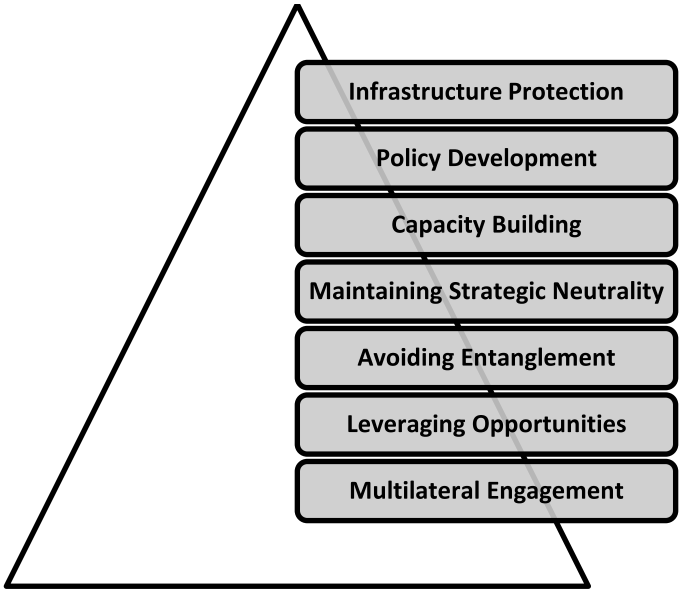
Theoretical Framework:

The study makes use of the following two theoretical formulations in seeking to understand the evolution of cyber enmity and how it plays out on the state of Pakistan:

Defensive Realism:

Defensive Realism provides a theoretical frame to look at how external cyber threats are perceived by Pakistan. A structural realist understanding of the world would lead the theorist to postulate that states are primarily concerned about their existence, and as such, seek to protect their territory and reduce the likelihood of foreign attacks against them (Stone, J. 2021). For countries such as Pakistan, this translates to developing a defensive posture against the increasing risks associated with the cyber competition between the US and China while preserving its cyberspace sovereignty (Yi, W. 2021).

Strengthening Cybersecurity Infrastructure



(Developed By Author)

Under the framework of Defensive Realism, selecting the security option whenever possible can be the best. For a country like Pakistan, it is explicit in dominance working on the establishing and sustaining thorough governance structure on cyber issues. So, Pakistan needs to protect critical areas like defense, energy, finance, and communication systems from cyber warfare threat because these are the areas largely being attacked by state and non-state elements in the much larger endeavors of achieving geo-political balance (Shahid, M. 2021). The first step has been taken towards protecting critical information infrastructure with the launching of the National Cybersecurity Policy (2021). However, updating, enforcing and ensuring world- wide cyber threats compliance, is necessary to mitigate new cyber threats in the future (Ahmed, H. 2024). To ensure the core focus on protection, Realism provides the perspective of training a competent workforce for cyber security preparedness, cyber attack and threat defense strategies integrating AI technologies, and even addressing the threats through cyber security namespaces (Smeets, M. 2022). Aiming for Strategic Inaction Pakistan is required to give its strategic neutrality so as to not get embroiled into the cyber rivalry of the US and China. This extends up to managing with both the powers without compromising its independence and optimizing the returns. Pakistan's closer relation with one of the super powers is likely to bring a risk of being threatened with cyber attacks or even economic sanctions and potential retaliation (Iqbal, S. 2020). To be specific, a stronger integration with China may trigger U.S. sponsored sanctions or even cyber operations aimed at assets like CPEC. On the other hand, a tilt towards the U.S. could lead to Chinese harassment of information systems or manipulations of vital systems (Khan, A. 2022). Strategic neutrality assists Pakistan in its relations with both the U.S., as well as China and in so doing helps Pakistani win technological and economic advantages. Engagement with China within the scope of the Digital Silk Road initiative may develop Pakistan's digital infrastructure while collaboration with the United States may offer beneficial opportunities in terms of sophisticated cyber defence mechanisms and international cyber cooperation (Li, Z. 2022). Furthermore, neutrality enables Pakistan to play the role of a mediator in the international debate on cybersecurity engagement. Through such bilateral forums, Pakistan can push for such global norms that underpin the preservation and promotion of cyber security stability and fair technology advancement (Abbas, T. 2023).

Offensive Realism:

In the anarchic form of the observation, the states are said to reside in a system, which at any given point is centered on the violent pursuit of dominion, which can be referred to as Offensive Realism. This theoretical lens also accounts for the more aggressive stances taken by both United States and China, when it comes to the cyberspace competition (Smeets, M. 2022). Cyberspace is at the service of both nations not only for the protection of their sovereignty but for their quest for global supremacy employing offensive cyber warfare, AI and information power (Segal, A. 2018). These developments make a significant contribution to the global regimes security and also pose considerable dangers and threats to third world countries especially Pakistan.

Empirical Evidence for Defensive Realism:

The cyber security policy was formulated in 2021 with the intention of minimizing threats to the critical infrastructure of Pakistan. The policy makes provision for protection of government and private sector's cyberspace assets with particular focus on defense, energy, and financial sectors. Measures for setting up Computer Emergency Response Team (CERT) and enhancement of cyber security literacy were also envisaged. More interestingly, the policy sets a target of reducing the cyber crime incidents by at least 25 percent by the year 2025. This target agrees with the doctrine of Defensive Realism, as Pakistan aims to defend its cyber presence and guard against external factors (Ministry of IT & Telecommunication.2021). In 2020 WAPDA, along with their strategic aid, suffered a series of cyber attacks, which caused a disruption in service. The malware used during the attacks was directed towards SCADA systems that assist in the energy distribution processes. Reports indicated that over 20% of Pakistan's grid management systems were temporarily shut down due to the attacks. This further emphasizes the need for stronger cybersecurity. Defensive Realism elucidates why Pakistan has meticulously placed so much effort on the safeguarding of its critical infrastructure from being weakened further, its economy and security for energy (Hussain, Z.2021) Specialist unit was set up in with a Pakistan army cyber attack budget of approximately 50 million dollars. The purpose of this unit was to counter cyber threats that could be directed at military and government networks. The Cyber Command has further ed over a hundred exercises of ongoing Hussein Z. Cyber threats in Pakistan Journal of Cybersecurity Studies. simulations to prepare for potential breaches. This is a clear reflection of Pakistan's alliance with Defensive Realism as it indicates that the country is making endeavors to conserve its interests and operational rights in an outrageous cyber space (Ministry of Defense. 2022).

Empirical Evidence for Offensive Realism:

In Operation Cloud 2014, China Used Offensives Reinforcement The only thing Left to Discuss China's MSS Support to The State Security Apparatus and Reincorporation of Wang ankow Mss Miss And Private Cloud HBT Point Problem Solving. Operation Cloud Hopper. El which China has stolen the data of illicitly sustained civil-military fusion activities. This work was conducted by the Chinese Advanced Persistent Threat (APT) group APT10 targeting Latin America on the Samp section 551.40 million dolar subverse korea provision of services particle exfiltrated over 1 TB of data (Symantec Threat Intelligence. 2019). The SolarWinds cyber spying case (2020) breach which is claimed to be orchestrated by Russia hacked into Orion, an IT management software used by over 18,000 businesses across the globe. Also, major US Organizations such as the Treasury Department and the Department of Security & Defense came under attack. As a result, a large amount of important information was leaked, the total damages caused by this attack are more than 100 million dollars. This is essentially a phenomena of Offensive Realism where Russia makes use of cyber measures to displace the attention of United States and help itself with geopolitical prominence.

Cyber Security During The US-China Conflict:

The conflict between China and US also includes advices from both sides to Pakistan to bolster its cyber security. The cooperation of Pakistan with China through the CPEC program has raised US concerns regarding cyber exploitation and data ownership. The US accuses Pakistan of aiding its ally China and forces Pakistan to adopt Western cyber controls while decrying the Chinese systems as threats to security. Similarly, Pakistan is viewed by China as a formidable ally in achieving its cyber and technological aspirations, Based on this collaboration, Pakistan has become the target of cybers attacks led by the US, including sanctions in retaliation on Pakistan.

Examining Pakistan's Cybersecurity System through the Scope of the Cyber Securitization Theory:

Cyber Securitization Theory enables a deep assessment of Pakistan range of actions with respect to cyberattacks while taking into consideration the growing US China competitive geographic environment. It observed what appears to be a parallel concerning the role of officials in the securitization process; these officials start the process by perceiving cyber risks as threats to national sovereignty and key infrastructures. Such a policy was adopted during the National Cyber Security Strategy Policy in 2021, where it was issued that sectors such as energy, defense and finance were key targets and cybersecurity is critical for the 'survival' of the country

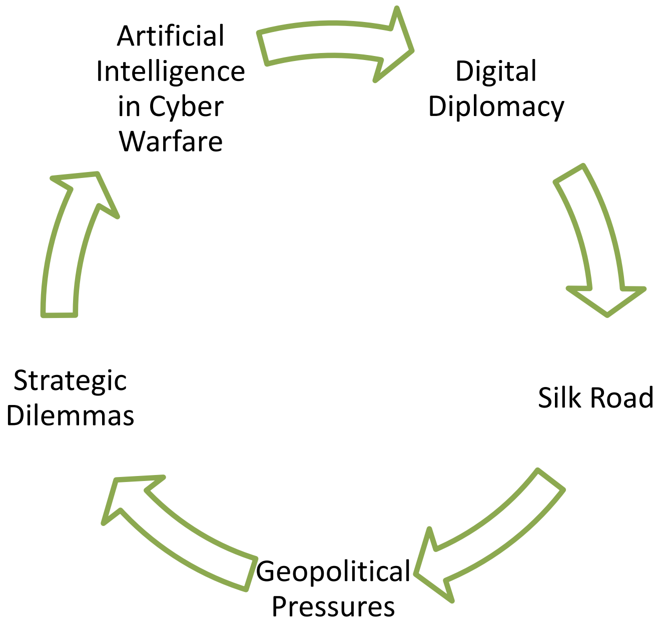
(Ministry of IT & Telecommunications, 2021). Along with this, the burgeoning of the Pakistan Army Cyber Command in 2022 demonstrates the further situs of this process alongside $50 dollars given for cyber protection of military and government networks (Ministry of Defense, 2022). Driven by the objectives of protecting Pakistan state, these countermeasures display the aspects of neo-constructivism that aim to secure the nation-state by providing comprehensive and well-defined boundaries to cyber security.

The vital referent objects in the securitization discourse in Pakistan are the critical digital sovereignty and the primary infrastructure. Such concerns are well-founded by evidence: cyber attacks on Pakistan Energy's grid in the year 2020 have damaged approximately 20 percent of operations which in turn shows the weaknesses of the regional infrastructure (Hussain, 2021). Pakistan also recorded a 300 percent increase of cybercrime cases between 2018 and 2921 which is yet another threat to national security (PakCERT, 2021). The ongoing projects and the corridor such as the China Pakistan Economic Corridor and the Digital Silk Road in addition to the above have also rendered the cyberspace security of the country worse as the Pakistan has to deal with the dilemma of adhering to US or Chinese technological principles (CPEC Authority, 2022). There is no doubt that these Chinese investments are very important for building the country's digital infrastructure, but they also leave Pakistan exposed to cyber retaliation from the USA, trying to get rid of China (Nye, 2021).

Pakistan has developed extreme measures ever since the threats arose including CECERTS and projects aimed at cutting down the cybercrime by 25 percent before 2025 (Ministry of IT & Telecommunication, 2021). Strengthening these ends Pakistan has allied with nations to hinder its own strategic control, for instance CPEC dependency on foreign technologies. The increasing rivalry between both US and China enhances Pakistan's will for a cyber securitization. China has placed its investments in digital infrastructure into strategic cooperation dynamics which exacerbate Sino-American friction (Symantec Threat Intelligence, 2019; Valeriano et al., 2018). The infiltration of Yin technologies constantly spying on US opens up a precession which Pakistan has to avoid fully securing itself while maintaining neutrality. By 2021 amnesty international raised alarms for citizens of Pakistan claiming an increase in the army stacked up threats to their civil rights and privacy (Amnesty International, 2021). By 2028 investing in CERTS along with the Cyber Command, commanding the last movement would ultimately slash civil rights_bounds while fragile arrangements were put in place. The Cyber Securitization theory sanctions Pakistan frame and answer cyber related issues addressing global threats framed as paramount issues. Appalled by the measures taken alongside them ensuring higher levels of security, this strikes balance alongside reverse mechanics for sustaining a nation over dependency on external technologies.

Cyber securitization theory has helped to articulate how Pakistan considers cyber threats as a legitimate security concern and how it addresses them under the global power structure. So, even as the policies that have been put in place bolster Pakistan's security capabilities, they raise critical issues regarding privacy, over-dependence on foreign technologies as well as the viability of Pakistan's approach in the fast changing digital age.

AI and Cyber Technologies as Tools of Influence



(Developed By Author)

In the case of AI and world domination, both the U.S. and China seem to be constantly fighting over who rules over cyberspace. Offensive Realism underscores the point that states use these instruments for global expansion and leadership politics (Nye, J. S. 2021). The use of AI enabled cyber weapons enhances the accuracy and range of cyber warfare of a state with a small chance of being caught. AI-enhanced malware, AI imaging, and AI-based predictive analytics have now secured critical areas of offensive cyber operations (Slayton, R. 2020). The U.S. and China also manipulate cyberspace for the purposes of digital propaganda. The Republic of China's Digital Silk Road strategy combines building essential structures with digital progress to engender dependency on partner countries and to increase China's clout (Li, Z. 2022). The same is true for the U.S. who uses cyberspace as a tool to advertise a global net while engaging in cyber conflicts to supersede Beijing's control of the gap (Clarke, R. A. 2020).

Consequences for External Countries:

Regarding Pakistan's geo-strategic environment, the cyber policies that the U.S. and China pursue are exceedingly aggressive and as result, creates significant pressures on Pakistan. Pakistan's involvement with projects such as the China Pakistan Economic Corridor (CPEC) and strategic partnerships with both the powers makes Pakistan prime for offensive cyber operations (Khan, A. 2022). Offensive cyber actions from either sides have the potential to bring down essential services, leak inviolable information, or destabilize Pakistan as an economy (Iqbal, S. 2020). Pakistan's competition with both US and China theoretically compels in making difficult strategic choices. To join on one power opens the likelihood of retribution from the other, and seeking non-alignment, risks offending both. For example, relationships might be constrained by increased pressure from the U.S. on Pakistan's government to adopt Western cybersecurity policies which would be frustrating because of their reliance on Beijing technologies (Iqbal, S. (2020).

Integration and Application to Pakistan

Technological Advancements
Strategic Neutrality
Enhanced Cyber Security Policies

(Developed By Author)

Integration with the global economy and reliance on technology makes Pakistan an arena of the US-China cyber-military struggle. As a state coping with two great powers, Pakistan has its own set of challenges and problems in such an information warfare arena. The armed defensive realism explains the stance of Pakistan looking out only for its own sovereignty and survival with vaster offensive policies of the US and China ever seeking to subdue Pakistan into servitude and forcing it into making changes and embarking upon strategies to safeguard its cyberspace (Iqbal, S. 2020).

1. **Enhanced Cyber Security Policies** Pakistan must focus primarily on security of its critical Infrastructure from potential risk of cyberattacks and cyber-espionage as well. Pakistan is in great need of all-encompassing cyber security policies in order to help shield these systems from both state and non-state sponsored attacks, it will be well protected from cyber crimes (Khan, A. 2022). Key sectors such as defense, energy, telecommunication and finance are major targets for cyber threats, Pakistan's National Cyber Security Policy is an introduction to creating a resilient ecosystem because it puts the effort to bring Pakistan into the digital space (Ahmed, H. 2024). Securing these infrastructures from state sponsored terrorism and attack is paramount. In concept, about the cyber regard of Pakistan security policy dated 2021, it manages to show some of the pervasive threats to its cyberspace. Furthermore, enhancing the international cooperation in any form contributes to deal with changing threats on the attention nation's defenders. The two dimensions provide a well-rounded rational for engaging both the public and the private sector in cyberspace resource sharing. This can help deal with shortfalls in resources to fight against cyber attacks (Abbas, T. 2023).

2. **Strategic Neutrality** Both China and US are the super powers and to say that Pakistan is caught in between these two powers would not be wrong but the real concern is how Pakistan can strike this balance between these two powers while at the same time preserving its sovereignty. (Ming, L. 2023). Leaving aside the American sphere critically restricts Pakistan's foreign relations for today's world is inter-dependent. For example, policies that strongly favor China can lead to a US-led international backlash targeted at CPEC projects flagged by Pakistan. So extending the reverse logic, allying with the US can invite Chinese cyber retaliation that aims at demolishing the critical infrastructure (Iqbal, S. 2020). This perfect neutrality gives Pakistan an ample opportunity to interact with both powers economically and technologically without getting caught in the arms race. Working with China under the Digital Silk Road initiative provides opportunities to improve digital infrastructure, while working with the US will enhance the cybersecurity environment (Abbas, T. 2023). Pakistan is able to portray itself as a neutral and responsible stakeholder in international roles looking to tackle issues of the cyberspace. Participation in multilateral forums puts Pakistan in a position to promote world standards aimed at stability, fair access to technology, and absence of violence in cyberspace (Khan, A. 2022).

3. **Technological Advancements** The two challenges that Pakistan faces today and are fundamentally intertwined is reliance on foreign technology and indigenously made, and what has to be emphasized is Pakistan's control over its digital landscape. To lessen dependence on foreign systems, Pakistan should focus on advancing indigenous technologies. Spending on research and development may drive the creation of new inventions in cybersecurity tools, artificial intelligence, and the field of communications (Ahmed, H. 2024). The advancement of the nation's technological capabilities can be achieved by collaborating with neutral countries and international bodies which have the capacity but do not attach geopolitical conditions. This strategy may mitigate the risks involved with overreliance on US or Chinese technologies (Abbas, T. (2023). It is critical to develop Pakistan's technical manpower in order to be able to keep up with technological progress. Measures for greater access of the population to computer screens, comprehensive training in cybersecurity, as well as skills in AI, can reduce the shortage of workforce and afford Pakistan an opportunity to thrive in the competitive international digital market (Khan, A. 2022).

Moving Towards Full Spectrum Deterrence: The US And Chinese Cyber Policy Towards Pakistan:

US and China's cyber policies necessitate Pakistan functioning under an environment of aggravated cyberspace hostility. This calls for a change from mainly being defensive and passive to going on the offensive which builds Pakistan's digital powers. In the context of advanced threats, the use of artificial intelligence in cybersecurity has considerable potential in threat detection and defense systems. With the help of AI powered tools, threat detection and incident response time can be automated and vulnerability prediction can be performed which will help Pakistan defend itself against the cyber attacks (Khan, A. 2022). Once developed, the use of offensive cyber capabilities as a deterrent can prevent enemy forces from attacking Pakistan. While remaining on the defensive, Pakistan, on the other hand, must demonstrate a resolve appropriate to the threat of cyber aggression and establish deterrence through the ability to respond to cyber aggression certainly (Shahid, M. 2021). Involving Pakistan's regional and global alliances in defense of military and economic aggression by the use of threat intelligence may assist Pakistan in predicting new threats. Engagement with neighboring countries and other neutral partners may help build a defensive network against cyberattacks (Abbas, T. 2023).

Pakistan's geographic location and dependence on digital systems make it an important actor in the US-China context of cyber warfare. Increasing the strength of its cybersecurity policies and remaining neutral while continuing to innovate is key to protecting Pakistan's sovereignty according to the principles of Defensive Realism (Slayton, R. 2020). Such adaptability however, also calls for proactivity when dealing with a hostile cyberspace in the form of AI based and cyber deterrence measures. Pakistan needs to find an effective balance between these approaches if it is to be able to effectively contend with the challenges of the digital age whilst safeguarding its interests (Iqbal, S. 2020).

References Articles Summary

American Writers

Joseph Nye – Managing Conflict Over Cyberspace: The Future of Cyber Power (2021):

Nye (2021) contends that the transformations in cyberspace power relations are altering the overall fabric of global politics focusing on the endowment of hard and soft power. Additionally, Nye explains how cyber tools help states as well as non-state actors project power, destroy critical assets or even spy on others. Nye proposes a set of codified global standards for violent states behaving in cyberspace to avert further escalation of sub conflict into war. He proposes multilateral arrangements as those that mitigate cooperation that can be used to neutralize ill will. His remarks point out the importance that cyber diplomacy has for the establishment of an international system, while considering the threats that countries put under national security protection.

John Arquilla – Future Perspectives of Cyber Warfare (2019):

Arquilla (2019) discusses about the certainty of cyber wars, how integrated systems become targets for attacks making their existence questionable. He suggests, netwar, where cyberspace makes traditional forms of conflict use residue obsolete. Arquilla analyses the past examples of cyber incidents and the implementation of previous historical events caring for the prevalence of defensive strategies. He suggests that threats from nations can be avoided by taking preemptive actions, for example, doing cyberspace deterrence. His article focuses on how offensive and defensive capabilities oriented towards cyberspace can be instrumental in winning wars making cyber warfare important while emphasizing the need in fighting for cybersecurity.

Richard A. Clarke – Cybersecurity and Cyber War: What Everyone Should Know (2020):

Cyber security and the plight of cyberspace war have raised the alarm on the race for stronger forms of technology as Clarke & eMite (2020) has noted. In 2019, NASA and Johnston & Sons set a record in a cyber warehouse, conducting only 70 virtual transactions across the total of 375 and claiming to have earned them a billion dollars. They have also heard from active duty members cyber hatred or retaliation or responding to the threats associated with cyber warfare, data theft, ransomware, espionage and loss of jobs that could compel one to think other than cyber space. Worries over cyber attacks directed particularly at critical infrastructures and what such consequences can mean for nation-states were reiterated by Clarke. Different types of public-private cooperation were endorsed in Armenia with the aim of targeting cyber threats. Clarke also pointed out that there should not be a disconnection between one set of people and creating and crystallizing the standards for cyber security such that development in technology outgrows conversely outgrows or out finances regulators. It is synthetic in Clarke's Part, what has been constructed is what is to be judi yet how social construction policies are freed about something devoted to cyber securedness contra social stability.

Bruce Schneier – Click Here to Kill Everybody (2018):

Schneier (2018) considers the threat posed by hyperconnected appliances which is sometimes called Internet of Things (IoT). He spoke against the decision of ignoring interdependencies of interconnected failures endorsing some kind of supervision. He further calls for the protection of people by means of building international regulations against cyber risks and creating secure design principles of technology. This work argues for the need to protect reason from fervor accompanied by progress.

Chinese Writers

Wei Zhao – The Rise of Cyber Sovereignty in China (2020):

According to Zhao (2020), the definition of cyber sovereignty should include the basic understanding of how China dominates its cyberspace's policies and practices. He further elaborated that the great firewall and other stringent policies were implemented in order to facilitate the protection of national interests and to propagate state agenda. According to Zhao the idea of cyber sovereignty is one of the key aspects of China's strategic objectives as it allows China to keep her data in a safe 'bubble' free from western or foreign intrusion while using the opportunities in technology to elevate her economy. China's cyber activism is one such measure that Yi indicates where he sees adverse effects for other countries particularly those intending to introduce para military structures and command policies to enhance their cyber capabilities.

Wang Yi – AI-Driven Cybersecurity: Challenges and Opportunities (2021):

Yi (2021) explores use of Artificial Intelligence in cybersecurity systems and the possibilities interconnected with it including risks. He maintains AI automated technology as useful in thwarting attacks by enabling identification of threat sources and allowing predicting potential sources. Zhi however cautions on the dual nature of AI, its application in targeting Japan in particular and conducting cyber operations in general. He terms for humanitarian principles on AI applications and points out why it's important to be open about AI projects, so they can't be abused.

Zhang Li – Contributions of the Digital Silk Road to Cybersecurity Cooperation (2022):

Li (2022) scrutinizes the participation of the Digital Silk Road initiative in the efforts at enhancing cybersecurity cooperation among the countries. According to him, there is a correlation between the investment that China makes in cyberspace and the creation of resilient networks. Li further mentions potential cybersecurity threats that come as a result of the initiative including concerns of potential data mining and espionage threat. The author finds that cooperation and trust is the most important aspect in order to be able to sustain progress over time.

Shen Xiaoyu – Cyber Deterrence in the Age of AI (2019):

Xiaoyu (2019) reports on China's cyber deterrence strategies, with emphasis on the cyber capabilities potential in the context of advances in AI. He looks at AI-enabled systems making the first strike and counter-strikes, emphasizing their role in the changing calculus of war. Xiaoyu notes that adequate deterrence will only be possible by caseating a significant level of deterrence and constant pursuit of advancement in sophistication and technology. He also remarks on the need to utilize international diplomacy to stem any chance of escalation and maintain stability in the digital space.

Pakistani Writers

Muhammad Shahid- Cybersecurity Issues for Developing Countries (2021):

Shahid (2021) highlights the cybersecurity issues that arise for countries such as Pakistan that are still developing. Tourism, workforce, reliance on human tools and outsourcing international services stand in the way of development as per the title. Shahid accentuates focusing on overcoming regional conflict and enhancing capacity across the region to build up cyber resistance. Furthermore, he cites bringing public attention to certain issues pertaining to the risks and effects of cyberattacks as an effective measure.

Ayesha Khan- Understanding the role of U.S.-China cyberspace confrontation for Pakistan (2022):

Khan (2022) looks to establish how the trade and technological competition between the US and China influences Pakistan's cybersecurity profile. The case study emphasizes the tension and the pressure exerted on Pakistan to take its eastern or western side whilst making sure it plays a neutral role. The key issues note shroud the fact that taking a proactive stance on engaging or investing into the country's core cyber structure is important to combat the protection of Pakistan's digital space. She also openly states the dangers that may arise from too much dependence on other countries in terms of technology.

Tariq Abbas – AI and Cyber Security, The Opportunities For Pakistan (2023):

According to Abbas (2023), in order for Pakistan to improve its cybersecurity focus on AI tech transfer and AI integration. This is evidenced by the fact which Abbas describes benefits related to AI in areas such as threat recognition, incident response, and vulnerability management. Abbas mentions issues such as evil deeds and other ethical issues, proprietary technology concerns and other issues which are obvious risk factors for deployment. He also talks about private-public collaboration in investment and research into local solutions as important.

Sana Iqbal – A Cyber Diplomacy in Relation To Pakistan's Security (2020):

Iqbal (2020) seeks to explain the increasing role that cyber diplomacy ought to play in the protection of Pakistan's digital space. She describes Pakistan's involvement in international bodies with the aim of influencing the international instruments of cybersecurity. Iqbal pushes for more effort on strengthening the partnership and involvement of nations on a trust -centric basis. In her work, she stately argues the consideration of cyberspace as a strategy form of warfare enhanced by diplomatic and propaganda efforts.

Incidents of Cyber Confrontation and AI-Driven Espionage:

Economic ambition and state goals have been enhanced by Artificial Intelligence and Concerns have been raised over use of cyberwars and AI driven espionage for hostile foreign policy. The next part seeks to ensure instances of cyber espionage include real instances of cyber warfare like Steamfitter, the hacking of the Microsoft exchange server violator which occurred anywhere between 2014 to 2024.

1. **Microsoft Exchange Server Hack (2021):** The Microsoft exchange server hack that occurred on the 3rd month of this year followed a group of Chinese state sponsored groups known as Hafnium accusing the nation of hacking American commerce. The cyber attack has left dozens of countries and corporates grappling with Africa being one of the most affected regions (Kumar, M. (2021) According to the hackers, delayed access to critical systems such as email was made possible by a nuclear weapon explosion or in this context, exploitation of cyber vulnerabilities. The breach was one of the most severe cyber attacks in the year 2021 as Microsoft claims that over 250000 email servicers around the globe were breached. Furthermore, the attack served to illustrate the level of sophistication that is now employed on cyber espionage techniques that target the most critical of the infrastructures (Kumar, M. 2021). Most alarming of all, is that the breach has impacted many ecosystems extending from healthcare to manufacturing and government as well. While this attack did not involve AI in itself, the targeting of specific organizations through zero-day vulnerability exploitation suggests that AI might be a tool of the future. And lastly, the new era tools will allow cyber scammers to easily explore opportunities by targeting flaws in vulnerabilities systems and, allow for vulnerabilities bleakness beauties to be rapidly identified. (Kumar, M. 2021).

2. **Operation Cloud Hopper (2014-2018):** Operation Cloud Hopper was a series of cyberattacks attributed to the Chinese state-sponsored hacking group APT10. In this case, the focus was on managed service providers (MSPs) and appropriate customers globally such as the largest technology companies, a number of government agencies, and defense contractors. Sophisticated approaches were employed by APT10 to penetrate cloud managed service providers (MSPs) and steal client sensitive information from them (Smith, B. 2019). The campaign might have persisted for more than a few years and was marked by numerous data breaches and even patent infringements across telecommunications and aerospace industries. China benefitted as a result by having access to business plans, some degree of technology and government secrets that could be useful in assisting their technological plans and geopolitical strategies. In this particular instance, AI could have been used to collect information from areas that the hackers, breached without financial information, resources and time delay. With a depressing amount of data at hand that was gained through emphasizing AI algorithms, the terrorists could have instead of all the

resources that had been wasted before, pinpointed the crucial information instead, thereby expanding the intelligence (Smith, B. 2019).

3. **SolarWinds Cyber Espionage (2020):** Towards the end of the year 2020, a breach became known in which there were attackers who were a part of a Russian cyber espionage organization on the other side. The cyber espionage organization targeted the software company SolarWinds by using a large scale of cyber attack (Goodin, D. 2020). They hacked into the company's Orion IT management software that was used by various important institutions including government agencies in all areas of the world. The attack, during which hackers operated undetected for several months, is viewed as one of the largest cyber espionage campaigns in history. Since the hackers were able to infiltrate Mandiant, the US Department of Homeland Security, the US Department of the Treasury, as well as private cybersecurity companies, their operation stands to be very significant. The SolarWinds incident emphasized how vulnerable the software supply chain can be and how severe the consequences of cyber espionage can be. The SolarWinds hack also demonstrates the increasing prevalence of AI and automation in cyberattacks (Goodin, D. 2020).

4. **The Pegasus Spyware Scandal (2018-2021):** Pegasus spyware created by the Israeli company NSO Group was offered to journalists, activists, politicians, and even dissidents on the International level. The spyware was able to use the loopholes in iOS and Androids to grant access to geo-tagging, targeted information on private communication access and many more. The campaign reached over 50,000 people cutting across various top people in Pakistan, India and many other countries. Pegasus emphasized the close relationship between AI, espionage, surveillance, as the spyware circumvented security targets and oversaw its targets using a machine learning algorithm in real time. Placing AI in use of spyware capabilities extended concerns regarding how far state and non state actors are able to be digital imperialists. AI has been applied in the production and use of spyware like Pegasus, which brings a new dimension to cyber espionage. AI works to improve the capability of the spyware to screen for security measures and counter, thus making cyber and information gathering relations more effective (Amnesty International, 2021).

5. **2024 Cyberattacks by Chinese Hackers to US Military contractors:** At the close of January 2024, Chinese hackers were ascribed a series of attacks that were directed to the US military contractors with the aim of stealing sensitive military technology and intelligence (Jones, S. (2024). The attackers employed phishing, malware and AI generated tools to breach networks to steal data from the targeted centers. This attack illustrates the growing tendency of AI enhanced cyber espionage aimed at defense capitals. Denial of access to critical military technologies is a threat to the national and integrated security as well as the international order. AI Espionage Tools- The involvement of AI within cyberattacks allows hackers to exploit mass datasets, distinguish key parts of information, while also redefining their tactics on the go making these attacks extremely efficient and almost impossible to track down (Jones, S. (2024).

Pakistan's Security Landscape

Pakistan's Cyber and AI Capabilities
The Role of U.S and China Digital Rivalry in cycles of Violence in Pakistan

(Developed By Author)

With the advancement of cyberspace and AI in today's world politics, Pakistan security matrix is also influenced by the digital factors and technology development. Pakistan's cyberspace and AI capacities are provided in this section in the context of the US-China Digital arms race and its implications for Pakistan's national security, AI driven cyber security, infrastructure security, and Diplomatic strategies.

1. **Pakistan's Cyber and AI Capabilities:**

As a result of the passivity of both state and non-state actors, Pakistan's cyberspace governance is in the process of transformation which has been longstanding. The country has made commendable achievements towards building a comprehensive and sophisticated national cyberspace through the following strategies: The 2021 Pakistan National Cyber Security Policy any critical information infrastructure protection framework, cyber security education, and strengthening the country's defense against cyber warfare. The policy recognizes that stakeholders must respond to cyber security threats in a coordinated manner and urges the public and private sectors to work together to improve the nation's cyber security. Cybersecurity Agencies: Pakistan has engaged the National Telecommunication and Information Technology Security Board (NTISB, 2021), which is a subordinate agency of the Ministry of Information Technology and Telecommunication and Pakistan Computer Emergency Response Team (PakCERT, 2021), among other institutions tasked with ensuring cyber security of the nation. They assist in the prevention, management and addressing cyber threats on the entire nation. This unique force's main function is to protect the country's cyberspace which has become the target of cyber-attacks, especially attacks against the key areas of energy, defense, and government. Pakistan's capabilities in Artificial Intelligence are very rudimentary in comparison to leading countries like America and china. Pakistan's growing interest in artificial intelligence mirrors that country's appreciation of the role of that technology in security especially in cyber security, that is in detection, prevention and action against cyber aggression (Ullah, F., & Khan, A. 2021).

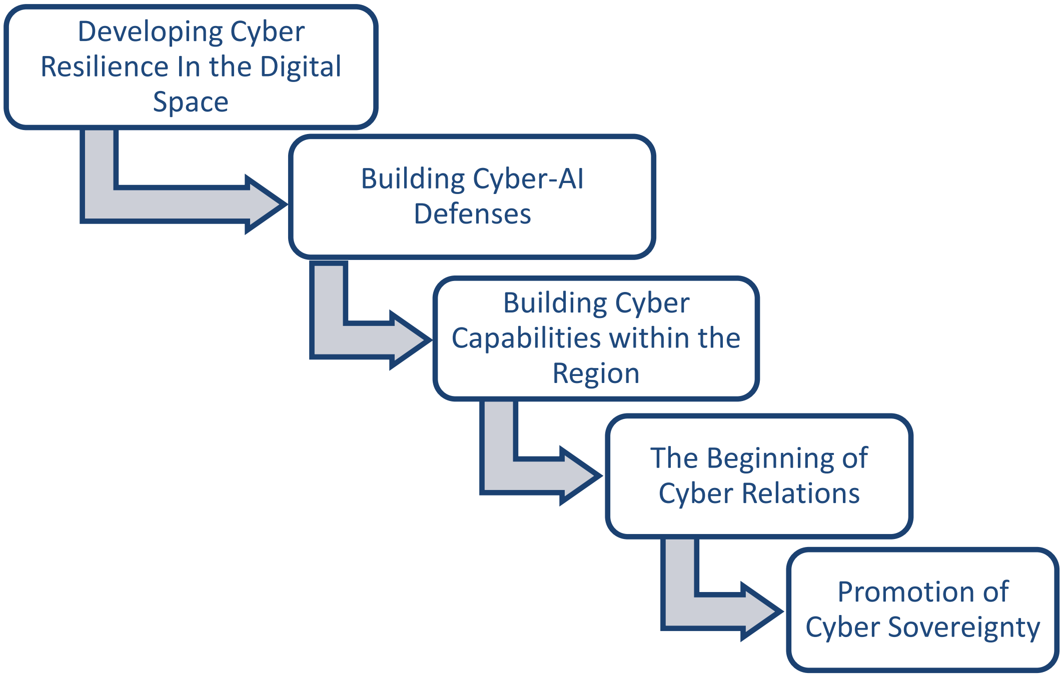
2. The Role of U.S and China Digital Rivalry in cycles of Violence in Pakistan:

The rise of power struggle between the U.S. and China has severe repercussions for the way Pakistan's cyber security system is designed, developed and where Pakistan stands in the world diplomatically. Pakistan has challenges at both the eastern and western flanks as both superpowers are in a race to digitally dominate the world which has repercussions on Pakistan's Nation Security and Cyber Security. (Hussain, Z. 2022).

Due to this strategic geographic location and cemented friendship with China, on a bitter rivalry between U.S. and China Pakistan is finding itself on the receiving end. In the event Pakistan builds deeper tech relations with China, it has the potential to become a cyber attack target by the U.S that would aim to dwarf Chinese global dominance (Khalid, R., & Ahmed, S. 2023). However, if Pakistan decides to maintain closer ties with the US it is likely to attract cyber retaliation from China on the contrary. There have been continuous efforts from both the US and China to use cyber space for espionage and to be able to obtain sensitive political, military, and economic information of each other (Nye, J. S. 2021). With China-Pakistan Economic Corridor (CPEC), Pakistan is becoming a strategic partner for both China and the US, and as a result, it becomes a target of such cyber espionage activities. Theft of state intelligence and key infrastructure assets and being exposed to cutting-edge AI-based cyber warfare is always a possibility. The US as well as China have also invested heavily in AI based warfare, which would increase the chances and intensity of future cyber attacks on Pakistan (Segal, A. 2018). AI based viruses and bots, automated scanning for weaknesses and later using bots to attack said weaknesses have already been employed. Pakistan would have the most difficulty fighting off such advanced digital warfare considering how recently AIs made their debut in the nation (Iqbal, S. 2020).

When it comes to the US and China tussle, Pakistan could choose to stay neutral on all matters relating to digital communication. This will be done by reaching out with both parties and addressing issues concerning that are important to them, such as counter-terrorism (Hussain, Z. 2022). In order to be able to that level of neutrality a dedication to the issue of protecting the territorial integrity of cyberspace as well developing autonomous cyber defense systems, so that cannot in itself prove to be easy because of the context in the earlier mentioned geo political frame. Pakistan may be subject to diplomatic and economic pressures (Iqbal, S. 2020). The Us and China could diplomatically and economically compel Pakistan in line with their respective cybersecurity frameworks. For example, the US could seek to influence Pakistan into adopting its cybersecurity standards and technologies, whereas China could provide Pakistan with access to its digital infrastructure and AI technology. Such pressures are likely to affect the cost benefit analysis of the concerned Pakistan's policymakers and make its diplomatic policy remain complex in the context of globalization (Khan, A. 2022).

Future Projections for Pakistan


Developing Cyber Resilience In the Digital Space
Building Cyber-AI Defenses
Building Cyber Capabilities within the Region
The Beginning of Cyber Relations
Promotion of Cyber Sovereignty

(Developed By Author)

Pakistan needs to invest more time and resources in building a comprehensive cyber security strategy so as to withstand the cyber threats in the future. Such strategy should include securing the development of local advanced technologies, creating public private environments, and strengthening the professional capacity of its cyber security manpower (Abbas, T. 2023). It would be crucial to apply AI technology in identifying and responding to cyber threats that are currently active and in real-time. AI based tools can assist in aggravating threat intelligence, streamlining vulnerability scans, and response time to incidents (Ahmed, H. 2024). Pakistan should look for partners in the region for threat intelligence exchange, investigations in cyber security, and integration of capacities against cyber offensive. Pakistan's active involvement in international discussions on cybersecurity has the potential to allow Pakistan to firmly establish its place in the international cyber governance structure. It is also about the establishment of rules aiming at the reduction of wars in cyberspace and the equitable distribution of cyber power, making sure there are no digital divides (Shahid, M. 2021). Pakistan needs to cut down its dependence on foreign technology by encouraging indigenous solutions and ensuring protection of its digital assets. This will require a properly articulated national plan which would include research expenditure, improving education and providing tax breaks for technology incubators. (Iqbal, S. 2020).

Conclusion:

The ongoing rivalry between the US and China in cyberspace has placed Pakistan at the focal point of a rapidly evolving digital arms race. This rapid conceptual shift demands new agencies and strategies that would tackle the challenges while exploring the opportunities. Being a part of the greater CPEC region, Pakistan also sits in a vulnerable position and has other important strategic options. The competition of two superpowers reshapes Pakistan's cybersecurity infrastructure and dictates its foreign policy moving the country in threats and alliances. Pakistan has become more and more susceptible to cyberthreats due to its geographic location and geopolitical importance. With capital and technology investments come over cybersecurity umbrellas, Pakistan has become the target of both the US and China. Wherever the American East meets the Chinese Northwest lies a Pakistan living on the brink of the Digital Silk Road, these two countries have technological competition. Both nations has geopolitically active, politically supports and influence Pakistan, one offering a promise of infrastructure then the other advanced worldwide cybersecurity tool. There are dangers in getting too close to one of them, revenge from the other would be the tangible product, therefore keeping quiet balance diplomacy while maintaining independence is essential. In terms of improving Pakistan's economy and self reliance they must focus on the development of their new cybersecurity strategy. Protective of critical infrastructure, public-private partnerships, cyber roaming investment management framework must also be developed. To decrease reliance on external technological sources, investment in research and development must focus on developing the country's technological capacities. Also, Pakistan must participate in regional and global forums to create a more balanced cyber norm and work to share threat intelligence. In this regard, it should be noted that proactive policy processes, strategic non-alignment, and international cooperation allow from optimal securing of Pakistan's sovereignty with the best possible exploitation of the technological progress. Adopting these strategies, Pakistan is able not only to handle existing cybersecurity risks but also to reorient itself as a resilient and agile actor in the changing global digital order.

References:

1. Abbas, T. (2023). AI and cybersecurity: Opportunities for Pakistan. Global Strategic Studies Review, 9(1), 45–60.
2. Arquilla, J. (2019). Cyberwar is coming: The future of state-sponsored hacking. Journal of Strategic Studies, 42(3), 345–359.
3. Buchanan, B. (2020). The hacker and the state: Cyberattacks and the new normal of geopolitics. Harvard University Press.
4. Clarke, R. A., & Knake, R. K. (2019). The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats. Penguin Press.
5. Nye, J. S. (2021). Managing conflict over cyberspace: The role of deterrence and diplomacy. Journal of International Affairs, 75(2), 33–56.
6. Segal, A. (2018). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.
7. Shahid, M. (2021). Cybersecurity challenges for Pakistan in the age of AI. Journal of South Asian Studies, 36(4), 211–227.
8. Slayton, R. (2020). Cyber power dynamics and the offense-defense balance. Journal of International Security, 45(1), 72–104.
9. Stone, J. (2021). Cyber deterrence in an interconnected world: Theoretical and practical challenges. Strategic Studies Quarterly, 15(1), 56–73.
10. Yi, W. (2021). AI-driven cybersecurity in developing countries: Challenges and solutions. Cybersecurity Journal, 12(2), 45–61.

11. Zhang, L. (2019). China’s emerging global data strategy: Implications for the United States. China Journal of Information Warfare, 14(4), 19–33.
12. Kumar, M. (2021). Microsoft Exchange Server hack: How China's Hafnium cyber attackers breached systems worldwide. The Hacker News.
13. Smith, B. (2019). Operation Cloud Hopper: How APT10 targeted MSPs for global espionage. Symantec Threat Intelligence.
14. Goodin, D. (2020). How hackers used SolarWinds to compromise Microsoft, FireEye, and the US government. Ars Technica.
15. Amnesty International. (2021). Forensic methodology report: How Pegasus spyware invades phones. Amnesty International.
16. Jones, S. (2024). Chinese hackers target US military contractors in sophisticated cyberattacks. Cybersecurity Journal.
17. Pakistan Computer Emergency Response Team (PakCERT). (2021). Cybersecurity readiness in Pakistan: A report.
18. National Telecommunication and Information Technology Security Board (NTISB). (2021). Strengthening Pakistan’s Cybersecurity: Annual Report. Government of Pakistan.
19. Ministry of IT & Telecommunication. (2021). National Cyber Security Policy 2021. Government of Pakistan.
20. Hussain, Z. (2022). Digital diplomacy and the US-China cyber rivalry: Implications for Pakistan. South Asian Cybersecurity Review, 10(2), 45–61.
21. Khalid, R., & Ahmed, S. (2023). Cybersecurity challenges for Pakistan amidst global digital hegemony. Journal of Cyber Policy and Security, 9(3), 88–102.
22. Nye, J. S. (2021). Managing power shifts in cyberspace: The US-China rivalry. Journal of International Affairs, 75(2), 33–56.
23. Segal, A. (2018). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.
24. Clarke, R. A. (2020). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
25. Ming, L. (2023). Critical Infrastructure Protection in China’s Cyber Strategy. Journal of Cybersecurity and Policy, 18(1), 65–78.
26. Li, Z. (2022). The Role of Digital Silk Road in Cybersecurity Cooperation. Journal of Cyber Studies, 15(2), 45–63.
27. Yi, W. (2021). AI-Driven Cybersecurity: Challenges and Opportunities. Tsinghua University Press.
28. Khan, A. (2022). The Implications of U.S.-China Cyber Rivalry for Pakistan. Pakistan Journal of Strategic Studies, 20(4), 12–30.
29. Abbas, T. (2023). AI and Cybersecurity: Opportunities for Pakistan. Islamabad Review of Technology, 8(3), 35–50.
30. Iqbal, S. (2020). The Role of Cyber Diplomacy in Pakistan’s National Security. Journal of International Relations, 17(2), 28–44.
31. Ahmed, H. (2024). Strengthening Pakistan’s Cyber Infrastructure. Karachi Journal of Policy and Security, 19(1), 41–58.

32. Zhao, W. (2020). The Rise of Cyber Sovereignty in China. Beijing University Press.
33. Xiaoyu, S. (2019). Cyber Deterrence in the Age of AI. Journal of International Security, 12(3), 23–40.