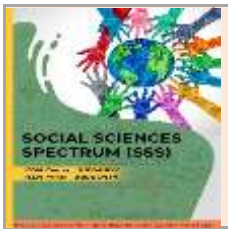

Social Sciences Spectrum

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

E-ISSN: 3006-0427 **P-ISSN:** 3006-0419
Volume 04, **Issue** 01, 2025
Web link:https://sss.org.pk/index.php/sss

Check for updates

Role of Artificial Intelligence and Cyberwar in America and China Influencing Pakistan

Salman Khalid
Research Scholar, Department of Political Science and International Relations, University of Management and Technology Lahore, Punjab, Pakistan
Correspondence: salmankhalid453@gmail.com

Article Information [YY-MM-DD]

Received 2024-12-06 **Accepted** 2025-01-20

Citation (APA):

Khalid, S. (2025). Role of Artificial Intelligence and Cyberwar in America and China Influencing Pakistan. *Social Sciences Spectrum*, *4*(1), 13-20. https://doi.org/10.71085/sss.04.01.191

Abstract

The efficiency of various contemporary processes depends highly on the implementation of artificial intelligence (AI) in the numerous tasks. While there is a significant set of benefits that AI brings to the table and while the results of AI integration can be a boost in productivity and launch of innovations, there is a set of issues that has to be taken into account. Moreover, AI and cyber space are combining the plethora of opportunities for many countries and adjusting the situation globally. The research work of this paper aims to undertake an analysis to unveil how realism principles inform policy choices of Pakistan particularly the opportunities and threats that result from the contemporary Cold War like competition between the United States and China within the digital frontier. Thus, this research aims to increase understanding of Pakistan's strategies and responses in relation to and on the basis of global cyber-geopolitics, including trends, strategic partnerships, and projections for the future. To this end, it seeks to map out the contingency at work in this fast-moving context and offer a sense of the systemic processes underpinning it, while shedding light on Pakistan's place in this emerging global order.

Keywords: Cyberwar, Artificial Intelligence, Cold war, Cyber geopolitics, Cyber security.

1. Introduction

There are a lot of developments in the field of artificial intelligence and cyber, the founders of the two countries are actively increasing their funding for AI and unmanned cyber weapons [1]. Literature review suggests that this new type of warfare in cyber domain might fundamentally transform regional security cape and draconically highlight the incumbent risks Pakistan has been exposed to being a part of South Asian map. Because of its role in the global power system and an intense reliance on technology imports, the country faces various issues related to the vulnerability of its vital infrastructures, economic sustainability, and its military forces [10].

Furthermore, the education AI systems have to follow five mandatory ethical requirements for well-being and safety in the workplace; trust, fairness; and, the rights to intellectual property, privacy and confidentiality [3]. Except for these general principles, ten additional principles have been enumerated. This study seeks to establish the relationship between AI, cyber operations and geostrategic competition and offer an agenda for effective policy for Pakistan to respond to these emerging threats. To understand these factors, there are three theoretical perspectives namely: structuralism liberalism and realism, which provide different perspectives of the various behaviors and actions in the system [7]. Realism always concentrates on power, security and self-interest and defines state's purpose in terms of strategy of USA or Russia, for instance [8]. For its part, liberalism puts emphasis on the role of international institutions, and cooperation as well as interdependence between states, supported by examples of Canada, New Zealand, and Norway. This paper used Structuralism, with a focus on Marxism and World-System Theory in a bid to explain how these power and economic structures influence state behavior as seen in France.

Artificial intelligence is the amazing possibility to copy human intelligence with the help of certain algorithms and further computer calculation abilities [4]. AI systems utilize the computational techniques like machine learning, natural language processing, computer vision to process the string of data, identify the feature and make sharply accurate determinations. AI technology involves designing computers with parallel processors so that they work like the brain and use particular algorithm [1]. Machine learning, one of the most popular subfields of AI, makes way for creation of smart machines Deep learning being a subcategory of machine learning employs preconstructed model architectures to compute data successfully.

Pakistan is at the moment in a process of experiencing the AI revolution in its banking system that is quite opposite to the one seen in developed countries [12]. Leveraging of Artificial Intelligence in those countries has been experienced in several important sectors like manufacturing, entertainment and media, education and healthcare boosting efficiency and decision making. However, the Pakistan share some problems and issues, which are security issues, ethical issues and issues related with the economical cracks, which may happen due to integration of AI [5]. However, it is gradually rising through the ranks in Pakistan in a number of domains of business and the economy. For example, in healthcare, Artificial Intelligence had shown to be priceless in helping hospitals track the productivity of the workforce to detail traits like attitude, emotion or behavior [18]. It also optimizes work performance while at the same time making the work environment more sensitive to the needs of patients thereby enhancing the quality of service handling a patient delivers.

Similarly, the sphere of cybersecurity is also growing more important as an umbrella of strategies for protecting networks, devices, software, and data from unlawful incursion and invasive activities [18]. In the modern world where countries fight in and through cyberspace it has become essential for countries to ensure they have well-developed cyber security measures and especially

as the two powerful countries of China and the United States of America use cyberspace as a war zone [2]. Both countries want to increase their influence on society while masking the negative effects of geostrategic rivalry on the outcome, revealing the essence of Sino-US confrontation in the digital world. While spreading their specific ideologies across the Internet, cyberspace remains the place of confrontation that influences relations on the global level [15].

AI is slowly becoming one of the essential aspects of the digital and military communication and planning among nations globally. There is still a major gap that has not been addressed to some extent on how governments use AI to extend the strategic influence at the operational level to military activities and informational warfare [13]. The objectives of this work will be focused on exploring some of the developed countries that have developed adequate AI systems and their assignments in cyber warfare or rather effects of these on Pakistan as a developing country [9]. In inspiration for this discussion, the analytical framework derived from realism is general in its philosophical application of both science and social science. In this context, the structural realism which can be referred to as neorealism, puts forward a very reasonable theory of international relations. This work maintains that power relations constitute the most fundamental form of force in interstate relations. First articulated by Kenneth Waltz in his seminal 1979 work, "Theory of International Politics," structural realism is further divided into two schools of thought: offensive realism, and defensive realism. Pivotal to this theory is the view that the ordering principle of the global system is anarchic while the distribution of capabilities particularly the number of dominant states in the system influences relations between actors. This framework will provide further insight into how AI might impact power relations especially in respect to cyber warfare and the case of countries such as Pakistan [9].

Cyber warfare transcends geographical boundaries and challenges conventional norms of conflict. It represents a novel battleground characterized by strategies that are often elusive and complex due to their inherently technical and sensitive nature [9]. In light of this, developed nations are increasingly focused on safeguarding their cyber-environments, and Pakistan is no exception to this trend. As we navigate the frameworks of neorealism and defensive realism, our analysis will center on Pakistan's unique perspective. The upcoming section will delve into prior research to provide a more comprehensive understanding of various concepts, including defensive realism, cybersecurity, and the intricate dynamics of US-China relations, as well as their implications for regional security. Additionally, we will explore the objectives and purpose of this study, aiming to elucidate the significance of these themes in the current geopolitical landscape.

2. Literature Review

AI systems are utilized across various domains, and their lifecycles encompass several stages: in research, designing, developing, deploying, and utilization. Because of this there are many definitions emerging as to what does qualify as an AI system. Experts have studied the trends of development of artificial intelligence and its incorporation into the cyber-space process, intensively revealing critical prospects for state practice and the maintenance of global security. The available literature is quite rich in pointing out the critical role of the new power forms and security perceptions in the AI-dominated cyber world. Major themes in key studies concern some crucial axis: AI, cybersecurity, and geopolitics [14].

The relationship between artificial intelligence (AI) and cybersecurity has become symbiotic, whereby AI impacts an array of current global politics and security policies as well as ethical questions. This review will provide a detailed evaluation of critical studies to understand various impacts of AI in cybersecurity [17]. It will explore diversified aspects such as the rising conflicts

that international relationships might stimulate due to new AI developments, the notion of 'cyber sovereignty', where nations try to control cyberspace, and the coming up of ethical risk management frameworks that are still struggling to strike the balance between creativity and caution when it comes to the act of developing and applying innovations in this field [16]. From this analysis, it is possible to comprehend the potential of AI for protecting the national interests and for facing the ethically problematic issues concerning further incorporation of artificial intelligent systems into security systems.

Some of the scholars like Tan in his work of 2023 and Khurshid in his paper of 2023 argue that artificial intelligence (AI) is radically shaping not only attackers' tools and tactics but those of defenders as well. Through the application of complex machine learning, different countries can be able to notice and avoid cyber threats hence boost their security [17]. However, this advancement helps where the AI enhances defensive mechanisms; at the same time, the cyber-attack profiling enhances their level, sophistication and automation of the attacks making the security landscape a bit more hills steep than hills flat. Ten and Sayankina (2023) prove that, on the one hand, AI complements cybersecurity, on the other hand, it brings significant risks and the task of protecting data and systems becomes a very difficult one. This changed perception of AI as both opportunity and threat creates a scenario that requires the development of a proper framework to improve, adapt and anchor AI to cybersecurity structures. The issue of AI interacts most clearly with the question of international competition, and, in particular, relations between the United States and China [2].

In this structural competition, Zhang (2021) asserts that AI is strategically significant in terms of positioning two sides as competing for technological supremacy. The US plan is the "National Artificial Intelligence Initiative Act" while China has the "Next Generation Artificial Intelligence Development Plan" that act as evidence of the two countries' aspirations to set the tone across the globe in terms of AI development [5]. This sibling rivalry does not stop at the technology war but brings into the world a badly divided technological, complicated world of divergent standards and shifting combinations. Furthermore, Zang's (2022) look into AI involvement in cyber espionage which resulted in the disruption of a sovereign state's function. These campaigns focus on important infrastructures and ideas; they augment geopolitical tensions; particularly for those countries that are in the middle of cyber wars [5] [13]. A good example is Pakistan which like any other developing world is faced with different hurdles when it comes to exercising cyber sovereignty. Limited resources and dependence on foreign technologies compound these challenges, underscoring the urgent need for nations to develop and implement localized strategies that can effectively address their specific vulnerabilities [9].

Moreover, Khan and Ahmed (2023) provide a rich understanding of USA-China cybersecurity competition toward developing countries. According to their research, there is a number of significant issues affecting these countries including overdependence on foreign technology, rising risks of cyber-attacks and lack of adequate policies for controlling Artificial intelligence (AI) systems [2]. In reference to countries such as Pakistan these sorts of contemporary international race AI presents many dangers comprising of; economic vulnerability, digital imperialism, and becoming an easy prey to worlds pressure. Similarly, in another aspect Zang (2022) goes to examine implications linked to the use of AI within the World Wide Web with special emphasis on the lack of universal regulation of artificial intelligence [6]. The absence of a well-coordinated comprehensive legal framework creates space for the AI development which in turn increases the risks in the areas already burdened with geopolitical tensions.

To this ethical debate, Ahmad (2023) avails himself in condemning reliance on AI in decision-making processes. Admitting that optimization is one of the areas that AI can help organizations with, Ahmad and Jahangir explain that over-reliance on such thinking often causes the human brain to stagnate and deteriorate, which weakens the top-level, critical-thinking elements. Cyber warfare, discussed by Ahmad and Jahangir (2023), is considered as a distinct domain which also differs from traditional warfare domain and type [9]. Examples of these experts provide a description of how both state and non-state actors strive to use cyber operations for gain through tactics such as sabotage, espionage, and any aim to disrupt a system. Similarly, Zhang (2021) and Shahriar (2023) have underlined the USA-China cyber conflict as decisive for the global cybersecurity [4] [5]. Their study proves how both countries use hi-tech tools to weaken each other's strategic standing while vying for technological dominance.

Meanwhile, Akram and Rehman (2023) expand on the details of how new technologies including AI shifted the context of cyber operations. One of the uses of machine learning and automation is to imperatively raise the bar and the volume of cyber threats as evidenced by the following factors [15]. However, as Mirza (2022) points out, there remains the issue of lack of international standards and treaties in respect to cyber policies. However, as Akram (2022) has pointed out there is lack of universally accepted normative structures and conventions on cyber-policies. Political and business enmities become barriers to cooperation in the management of the Internet space, which remains fragmented and insecure [16].

Essentially, the ethical considerations of cyber warfare are receiving a lot of attention in this line of literature. Ahmad (2023) appropriately puts forward several questions such as the ability of wrongdoers to penetrate user's data and privacy, the probability of hurting the innocuous civilians, and the possibility of the conflict escalating due to some misidentification or flawed estimation of the adversarial cyber-operations [9]. They illustrate why currently the need for fundamental approaches aimed at preventing and punishing misconduct in cyberspace is so essential. Zhang continued this perspective further and from a defensive realist point of view, Hunter 2021 argued that security-based approach is the only one that makes sense of state actions in the digital world [7]. They give warning of power-maximization strategies, noting that such behaviors can only lead to disequilibrium in the international system and cause conflicts [6]. However, they argue that states ought to pursue a collective security approach by moderation of cyber operations leading to responsible state behavior.

Additionally, with somewhat contrasting views on the roles and impacts of artificial intelligence (AI), cybersecurity, and international relations in the examined literature, it is now necessary to define their interconnections. It is now clear that technology provides first-rate benefits; however, it is also an explanation of complex ethical, legal, and strategic challenges that are not amenable to dismissal. The current competition between the USA and China in Cyber space is the best example of how AI enhanced Cyber capabilities are shaping the relations, more often at the emerged new world order discomfort of developing nations. This situation clearly depicts the need for collaboration and inclusive policies and strategies that will promote the sharing of the AI and cybersecurity rewards and risks with countries of no regret the more the world goes technical.

3. Research Objectives

The first one objective is to centers on providing a broad picture of cybersecurity in Pakistan; any consequences it has is also included under this objective. As a country with heavily growing digital infrastructure, Pakistan becomes even more vulnerable to cyber risks in regards to its economy, protection, and security. The research is intended to assess the current position of cybersecurity

frameworks and their weaknesses in both the governmental and commercial areas as well as the ability of key infrastructures to counter cyber-threats. This study aims at evaluating the existing policies and reaction procedures of Pakistan towards cyber-threats uncovering understanding on the implications of cybersecurity threats on the Pakistan's societal and economic frameworks. Thus, while identifying areas where such research is lacking, the study will seek to illuminate crucial stages that would help enhance Pakistan's cyber-protection.

The second one objective goes into a focus on how the cyber-competition between the US and China influences the Pakistan's political climate in terms of cyberspace. Pakistan being an emerging country in the region directly faces the consequences of actions of two super powers in cyberspace. The paper assesses the emerging trend in which the conflict between the US and China goes beyond the cyber-arena into forcing the desire of other nations like Pakistan into joining one camp or the other. This paper explores the nuances of technology imports; technology transfer; and how Pakistan has been shaped by infrastructure, development loans, arms imports, and strategic partnerships with both China and the USA. By dealing with these influences, the study intends to evaluate in which measure Pakistan is affected in the economic, the technological and the political sphere by this cyber-rivalry.

The last one objective examines the possibility of the measures that may indeed be adopted by Pakistan to stand up to the consequences of current US-China cyber-espionage without losing sovereign control over its own national interests. It underlines the policy that contains one in the sphere of military conflicts, with the non-interconnected interest clash of the two superpowers. This paper also underlines the potential further priorities of the capacity building processes such as the encouragement of the indigenous knowledge systems in technologies, strengthening of cybersecurity measures in the governmental policies and the balanced approach in the international cyber-politics.

4. Conclusion

The views about precisely how Pakistan may or may not become involved in world conflicts are indicative of the multifaceted approach to geopolitics. The nation's participation will also depend with how it will balance power diplomacy within the international arena, form symbiotic relationships with other nations, and enhance its cybersecurity. Ever since the incorporation of the Information Age and computing technology as tools in warfare, intelligence and cyberspace are key revolutionary forces defining the modalities of the relationship between the state and its competitors, partners, and adversaries. This is well illustrated by the continuous cyber-space confrontation between the U.S and China; the competition over new technologies demonstrates their potential of reshaping power relations in the world. This competitiveness is also become the factors and threats to the countries like Pakistan where they can gain benefits but also can lose too.

On the other hand, Pakistan may benefit in improving her cyber-security capacity and improving its digital base from technology offered by these superpowers. It could also help the nation to move forward with development during the current digital age. At the same time, Pakistan has to be more cautious because reliance on both states has its drawbacks, for example, exposure to cyber threats, or dangerous geopolitical shifts because of too close cooperation with one of the blocs against the other. These are the questions regarding the security and functionality of cyberspace that Pakistan needs to answer to defend its national interests in the ever-growing, but hostile environment. In particular, the challenges of inclusive governance, the use of technologies and artificial intelligence, and the creation of effective cybersecurity systems will be highly significant in the digital area. These measures will assist in containing possible dangers while ensuring that everyone involved in this technological evolution will derive as many advantages as possible leading to the general protection of the whole world's digital sphere.

References

Ertel, W. (2024). *Introduction to artificial intelligence*. Springer Nature.

Tan, E. W., & Sayankina, S. (2023). Cyberwarfare and the Weaponization of Information in US–China 21st-Century Geostrategic Rivalry. *Pacific Focus*, *38*(2), 180-209. https://doi.org/10.1111/pafo.12233

Mir, M. M., Mir, G. M., Raina, N. T., Mir, S. M., Mir, S. M., Miskeen, E., ... & Alamri, M. M. S. (2023). Application of artificial intelligence in medical education: current scenario and future perspectives. *Journal of advances in medical education & professionalism*, *11*(3), 133. doi: 10.30476/JAMP.2023.98655.1803

Mannuru, N. R., Shahriar, S., Teel, Z. A., Wang, T., Lund, B. D., Tijani, S., ... & Vaidya, P. (2023). Artificial intelligence in developing countries: The impact of generative artificial intelligence (AI) technologies for development. *Information Development*, https://doi.org/10.1177/02666669231200628.

Zhang, T. (2021). Was Weber Really Wrong? A Comment on Some Recent Empirical Studies on Economic Growth. *Max Weber Studies*, *21*(2), 203-212. 10.1353/max.2021.0022

Zhang, T. (2022). Ethics and Society: A Theory of Comparative Worldviews. In *The Routledge International Handbook of Sociology and Christianity* (pp. 177-190). Routledge.

Hunter, L. Y., Ginn, M. H., Storyllewellyn, S., & Rutland, J. (2021). Are mass shootings acts of terror? Applying key criteria in definitions of terrorism to mass shootings in the United States from 1982 to 2018. *Behavioral sciences of terrorism and political aggression*, *13*(4), 265-294. https://doi.org/10.1080/19434472.2020.1762108

Hunter, L. Y., Albert, C. D., Henningan, C., & Rutland, J. (2023). The military application of artificial intelligence technology in the United States, China, and Russia and the implications for global security. *Defense & Security Analysis*, *39*(2), 207-232. https://doi.org/10.1080/14751798.2023.2210367

Ahmad, S., & Jahangir, J. (2023). Cyber Warfare: Emerging Non-Traditional Threat to Pakistan's Security. *Pakistan Horizon*, *76*(2), 39-58.

Ahmad, S. (2021). China-Pakistan Post Covid-19 Economy and Progress on China Pakistan Economic Corridor (CPEC). *UW Journal of Social Sciences*, *4*(2), 99-116.

Azad, T. M. (2020). Understanding The International Propaganda Patterns Against Pakistan. *Institute of Regional Studies Islamabad*, 209-233.

Zaheer, M. A., Ikram, M., Rashid, S., & Majeed, G. (2023). The China-Russia strategic relationship: Efforts to limit the United States' influence in Central Asia. *Stosunki Międzynarodowe–International Relations*, *3*(3), 3. (https://doi.org/10.12688/stomiedintrelat.17631.1)

Simons, G. (2023). 9 Geopolitics in the Age of Social Media: The Struggle for Influence on Ukraine. *Rethinking Warfare in the 21st Century: The Influence and Effects of the Politics, Information and Communication Mix*, 246.

Flint, C. (2021). *Introduction to geopolitics*. Routledge. https://doi.org/10.4324/9781003138549

Akram, M. S., Mir, M. J., & Rehman, A. (2023). Dimension of cyber-warfare in Pakistan's context. *Journal of Positive School Psychology*, *7*(6), 82-94.

Mirza, M. N., & Akram, M. S. (2022). 3-Cs of Cyberspace and Pakistan. *Strategic Studies*, *42*(1), 62-80. https://www.jstor.org/stable/48732344

Khurshid, T. (2023). The Impact of Artificial Intelligence Militarization on South Asian Deterrence Dynamics. *BTTN Journal*, *2*(2), 134-150. https://doi.org/10.61732/bj.v2i2.76

Iqbal, S., & Tabeer, S. (2024). Digital Strategic Autonomy in South Asia: Artificial Intelligence and Cyberspace. *Journal of Security & Strategic Analyses, 10*(1), 72-86. https://doi.org/10.57169/jssa.0010.01.0300