ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 04 No. 01. July-September 2025.Page#.64-76
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

The Digital Battlefield: A Comparative Analysis of AI-Driven Cyber Warfare in the U.S. and China and Its Implications for Pakistan's National Security

Uswa Khalid
Mphil Scholar International Relations, University of Management and Technology, Lahore

Abstract
The study explores the deepening U.S.-China competition in cyber warfare driven by artificial intelligence and its strategic consequences for Pakistan. Relatively smaller states such as Pakistan are forced to adapt and maneuver within a digitally contested security landscape, which is shifting due to the integrated use of AI innovations in military and cyber domains by both superpowers competing with one another through differing models of innovation, governance, and deployment. The research focuses on the U.S. and Chinese rival cyber strategies comprehensively around their doctrinal, operational, technological differences along with contextualizing them into the scenario of India-Pakistan conflict 2025 where AI-enabled warfare was crucial. Using offensive realism as the framework, the research highlights the impacts of structural forces that compel Pakistan to take advantage of Chinese technological backing while simultaneously being exposed to geopolitical-strategic dependency risks. Qualitative methods were used to identify policy gaps in response to dual vulnerabilities the urgent need for development that will lead to national resilience within ethical bounds and the lack of self-reliance in AI and cybersecurity drawn from literature reviews, policy analyses, and expert interviews. The conclusion outlines strategic autonomy as well as investments stressing proactive governance concerning digital design frameworks. It emphasizes cross-sector synthesized approaches responding to rising threats mounting at accruing strained interdependence framing peripheral states from dire subordinated status onto clear vision revealing new frontiers waiting exploration having transformative potential metamorphosing states like Pakistan sidelined into pivotal players drawing direct contribution shaping discourse on global asymmetrical dynamic rivalry headlined south-east continuum STEM as tributary fueling supers.

Keywords: *Artificial Intelligence (AI), Cyber Warfare, U.S.-China Rivalry, Pakistan National Security, Offensive Realism, Military-Civil Fusion, Strategic Autonomy, Digital Sovereignty, AI Ethics, Geopolitics*

Introduction

The Digital Battlefield: AI-Powered Cyberwarfare between the U.S. and China and Its Implications for Pakistan's National Security

The world that we live in today is very different due to a paradigm shift in the way wars are fought. Increasingly, the classical concept of conflict has been replaced with other forms of warfare that deal with programs, lines of code and digital representations. The role of artificial

intelligence (AI) has become the main factor of the new age of war as far as the military and strategic priorities are changing towards cyberspace. The use of AI in cyber warfare or AI-driven cyber warfare is radically transforming the nature of state defenses and power projection as well as dealing with enemies.

The artificial intelligence allows automating and increasing the speed of cyber operations, changing all stages, including reconnaissance to the implementation of attacks. Machine learning algorithms are now able to automatically identify the vulnerabilities on the systems, create personal exploit, and steal sensitive information with the precision and stealth. Such a scale of velocity and complexity renders more and more the old methods of defense obsolete. In this way, AI does not just make cyber capabilities better; it transforms them and introduces a time when war may be commonly approximate, immediate, and asymmetric.

The United States and China are two world powers that are at the center of changing this phenomenon. The two countries understand the strategic importance of AI and are doing a lot of development to gain a military and cyber advantage. Nonetheless, their patterns of integration of AI are hugely different. The U.S. model is based on the idea of innovation of a privately-owned sector, transparent cooperation and world leadership. With Third Offset Strategy and the creation of such offices as the Joint Artificial Intelligence Center (JAIC), the U.S. aims to preserve technological superiority. The American cyber doctrine, in particular, through its U.S. Cyber Command (USCYBERCOM) has been promoting the proactive strategy to cyber adversaries, which instilled its so-called, defend forward concept where the adversaries are neutralized before their attacks are realized.

Conversely, the Chinese form of cyber sovereignty advocates absolute governance, state-driven research and convergence of industrial and military forces through its Military-Civil Fusion strategy. The vision was envisaged in the 2017 "New Generation Artificial Intelligence Development Plan" the goal of which is to achieve the status of the world leader in AI by 2030. Such extensive engagement of the Chinese state with civilian tech giants, along with its purported relationships with non-state cyber actors, has created a powerful cyber landscape: not only an opaque, offensive, and staunchly nationalistic one, but also one that is linked to and can be deployed at the behest of ordinary, mundane citizens. Whether they are in the form of global cyber espionage activities or AI-rooted surveillance measures, the Chinese plan aims at gaining long-term superiority in both virtual and physical spheres.

With this escalating competition between the U.S. and China in the field of technology, Pakistan is on a dicey strategic fork. Lying at the interchange of South Asia, the Middle East, and Central Asia, and a long-time having a complicated security relationship with India, national security in Pakistan is becoming drawn in the rapidly changing cyberspace game of cyber power and AI militarization. Although it does not have the resources and depth of technology as the major powers, Pakistan cannot be just an observer. It is already a indirect player in the digital competition, either in bilateral alliances, in digital dependencies, or even in the peripheral effects of superpower cyber warfare.

This new reality was graphically illustrated in the conflict with India in May of 2025. Against the backdrop of a traditional military disadvantage, Pakistan was forced to use AI-facilitated cyber and information warfare, in which the Chinese technological assistance was partially involved.

These attempts provided tangible tactical benefits such as interference with the Indian communication, leakage of information, and discretionary disinformation programs. But it was also during the war that the flaws of Pakistan were revealed most notably was the fact that they relied too heavily on outside technological provisions and indigenous competency was undeveloped.

It is this duality (between opportunity and vulnerability) that characterizes the current cyber position of Pakistan. On the one hand, the cooperation with China provides entering into the world of technology and the mutual strategic interests. On the one hand, such dependence reduces strategic independence and raises the threat of geopolitical involvement, especially across China as the United States and its other member countries monitor Chinese cyber expansionism with caution. Moreover, Pakistan is ill-equipped with its infrastructure, research and development system, policymaking mechanism, and cyber governance systems to deal with the sophistications of AI-intimidated warfare.

These risks are further exacerbated by India leading parallel AI and cyber warfare as well. In close contact with the U.S. and Silicon Valley, India is fast entering into the domain of AI in national security. Indian cyber units have engaged in offensive operations into Pakistan networks and this has highlighted the increasing disproportion to regional cyber capabilities. Such trends imply that Pakistan should seriously reexamine its doctrine of national security and change its vision to be more inclined to grasp the current trend that is a change towards the usage of technology in enhancing national security instead of relying on conventional patterns of military development.

The study aims at filling this gap. Specifically, it undertakes a **comparative analysis of AI-driven cyber warfare strategies** in the United States and China and explores their implications for Pakistan's national security. The study is guided by four key research questions:

1. How do the United States and China differ in their use of AI in cyber warfare, and what are the defining features of their respective strategies?
2. What are the strategic risks and potential benefits for Pakistan in navigating this technological rivalry?
3. How did the May 2025 conflict with India illustrate the operational impact of AI-driven cyber warfare on Pakistan's military effectiveness?
4. What policy and technological steps must Pakistan take to reduce vulnerabilities, enhance resilience, and develop autonomous capabilities in this domain?

By answering these questions, the study aims to fill a critical gap in both academic scholarship and policy discourse. While much has been written on U.S.-China cyber competition, far less attention has been given to how this rivalry influences **secondary and tertiary states**, particularly in volatile regions like South Asia.

The **significance** of this research lies in its policy relevance and timeliness. As AI becomes an indispensable tool of statecraft, countries like Pakistan must craft strategies that balance external partnerships with internal capacity-building. The proposed study is expected to add value to the developing sphere of AI and national security, as it provides evidence-based information and strategic advice to the policymakers of Pakistan, military planners, and the cyber specialists.

Moreover, the research is relevant to the international relations and even cyber diplomacy in general. The U.S.-China rivalry in the field of AI is not a two-sided game, it is a reconfiguration of powers on a world wide scale into the digital sphere. It is within this climate that countries that are in between will have to tread cautiously, dynamically and strategically. Through a case study of Pakistan which has been in the habit of geopolitical balancing and asymmetric warfare, the study is useful to other countries in a comparable position on the technological periphery but with vulnerability.

The comparative case study analysis is coupled with qualitative content review as the methodological approach of this research. Based on the open-source intelligence, the defense white papers, the policy documents, and interviews of domain experts, it systematically analyzes the processes of the implementation of AI in the cyber doctrines, military organization, and policies in digital areas in both the U.S. and China. Particular focus is placed on recent wars, particularly the May 2025 conflict between India and Pakistan so as to base the analysis on real life implications.

Finally, with the conflict getting into the realm of cyber warfare and AI taking the center-stage in the military strategy, Pakistan cannot sit on its heels and needs to make the right decisions promptly. Otherwise, it can incorporate strategic vulnerabilities that can be disastrous in future wars. In contrast, sound investments on AI, strong policy change, and international multi-dimensional relationships can make Pakistan a safe state, which is capable of exerting its sovereignty in a hazardous cyberspace.

Literature Review:

Over the past years, the combination of artificial intelligence (AI) and cyberwarfare has become one of the characteristics of international strategic struggle, especially between the US and China. The rivalry between the two countries is determining the future of international security as the two compete to use AI to acquire both offensive and defensive cyber capabilities. This AI-empowered cyberwarfare has been an increasingly analyzed cyberwar scenario when seen in relation to geopolitics, and the consequences of its effects on third-party countries are developing interest. Pakistan is a nation that, with its alliance with China and catastrophic relations with India, is in a critical point where the impact of digital militarization can be impending and fundamental. The literature review condenses the most eminent works by academics, policymakers and think tanks that examine shifting AI-cyber nexus between China and the U.S., and evaluates its impact on Pakistan national security.

The Rise of AI in Cyberwarfare

Accounted by AI, the development of cyberwarfare has significantly been advanced. According to Singer and Brooking (2018), AI makes cyber operations scalable and faster since it allows automatic intrusion, real time threat detection, and adaptive malware. AI tools are also able to take advantage of vulnerabilities at large scale which renders them to be suitable during offensive cyber operations. Moreover, according to Brundage et al. (2018), AI enables quicker and more efficient lifecycles of the cyber-attacks, particularly in a zero-day exploit and lateral movement within the networks.

Horowitz et al. (2020) explain how the presence of AI in cyber operations decreases decision-making time and confuses the distinctions between holding espionage activities during

peacetime and the course of battle. This has triggered great powers especially the U.S. and China to integrate AI in their cyber doctrine. The dual-purpose nature of AI (both civilian and military) poses another challenge in regulating these technologies, monitoring their use, and attributing cyber actions, although it enhances the strategic confusion around cyber activities.

The U.S. Approach to AI-Driven Cyberwarfare

The United States has gone a long way in incorporating AI in its defense/Cyber infrastructure. The Joint Artificial Intelligence Center (JAIC) of the U.S. Department of Defense was created in 2018 to manage the development of AI between services. Project Maven is one of the examples to show that the U.S. is aimed at the use of AI to analyze intelligence and prioritize targets (Allen & Husain, 2017). Despite the fact it is mainly about image recognition, the real-time cyber threat intelligence implications of Project Maven are being more acknowledged.

The recent research points out the efforts of the U.S. to apply AI to predictive modeling of threats. Kania and Laskai (2019) state that AI allows seeing cyber threats in advance and encounter fewer needs to rely on human analysts. In addition, the U.S. Cyber Command (USCYBERCOM) is said to incorporate AI to protect the critical infrastructure, perform penetration testing, and mimic the actions and responses of adversaries (Schaub & Maurer, 2021).

Nevertheless, the same researchers warn also on the extreme use of an autonomous system. According to Binnendijk et al. (2021), the identified risks include escalation caused by false positives or misunderstanding the nature of the incident by an AI in the cases of ambiguous cyber incidents. The ethical aspects of autonomous cyber responses are not fully developed in the U.S. doctrine, evoking concerns about the responsibility in the AI-enhanced combat.

China's Strategic Use of AI in Cyber Operations

The Chinese strategy regarding AI and cyberwarfare is characterized by the so-called "Military-Civil Fusion" (MCF) strategy according to which state and commercial sectors are obliged to collaborate in order to accelerate military AI. In the 2017 "Next Generation Artificial Intelligence Development Plan" (Ng, 2020), the Chinese government considers AI as one of the spheres of critical leadership on the global scale. Researchers like Creemers et al. (2018) believe that China uses AI both in strategic and tactical cyber operations through state-affiliated organizations such as PLA Strategic Support Force (PLASSF).

The Chinese cyber actors, particularly APT groups funded by the state, are said to implement AI to enhance scouting, execute phishing campaigns automatically, and steal data of high-profile targets (Rid, 2020). Other examples of applying AI to the cyber doctrine of China can be observed through the strategic use of deep fakes and disinformation, which are used to influence the masses favorably and compromise enemies on the inside.

Moreover, scholars mention that China invests into the development of AI-empowered surveillance tools such as facial recognition systems, behavioral analytics, and behavioral analytics are used not only to control people within China but also can be deployed as foreign cyber capabilities. Greitens (2019) notes that this transformation is being exported by China because its digital authoritarianism based on AI is being globalized via projections such as the Digital Silk Road.

U.S.–China AI Cyber Rivalry and Global Security

The strategic rivalry between China and the U.S. has ceased to confine itself only to traditional fields but develops in the digital arena more and more frequently. According to Lindsay and Gartzke (2020), cyber conflict is naturally covert, and this combination of the features creates increased risks of miscalculation and escalation when using AI. The two powers' competing visions—democratic digital governance versus centralized control—are reflected in their cyber operations and AI ethics.

Recent literature points to the weaponization of critical infrastructure as a key front. Clarke and Knake (2019) argue that AI-enhanced cyber tools could disrupt power grids, telecom networks, or financial systems, with real-world kinetic consequences. In this context, non-aligned and third-party states are at increased risk of collateral damage or being drawn into conflicts via cyber dependencies.

Pakistan's Cyber and AI Capabilities: A Nascent Framework

Pakistan's engagement with AI and cyber defense has evolved slowly compared to global trends. As noted by Ahmed and Sheikh (2021), Pakistan's cybersecurity policies have traditionally been reactive, lacking integration with emerging technologies. However, the formation of institutions like the National Center for Cyber Security (NCCS) and the establishment of the Pakistan Computer Emergency Response Team (PKCERT) indicate a growing recognition of cyber threats. In recent years, Pakistan has taken initial steps to adopt AI in security and defense sectors. According to the Center for International Strategic Studies (CISS), Pakistan has initiated projects under its national AI policy to integrate AI into surveillance, border management, and decision support systems. However, scholars argue that these efforts remain fragmented and under-resourced (Khan & Javed, 2022).

Implications for Pakistan's National Security

Strategic Dependencies and Cyber Vulnerabilities

One of the key themes in the literature is Pakistan's growing reliance on Chinese digital and defense technology, including AI-enabled platforms. This dependency raises questions about digital sovereignty and potential vulnerabilities. Rabia Akhtar (2022) points out that an overdependence on China's AI systems could expose Pakistan to backdoors, surveillance, or coercive leverage during diplomatic crises.

At the same time, Pakistan's limited integration with Western digital ecosystems, due to geopolitical alignments and export controls, reduces its access to diversified and interoperable AI systems. Thinking scholars warn that such digital separation would weaken the capacity of Pakistan to counter the cyber-related threats by either of the two powers.

Regional Escalation and Arms Race Dynamics

Cyberwar AI also in-security at the South Asia region. According to the research conducted by Bajoria and Lalwani (2021), the swift integration of the AI-equipped military systems in India stokes apprehensions in Islamabad, which might give rise to an arms race. Both nations are considering more autonomous swarms of drones, decision-making supported by artificial intelligence and cyber attack capabilities.

By introducing AI into the means of and mechanisms of deterrence, the stakes of going to war may become cheaper or lead to unwitting conflict. As an example, electronic early warning

detectors or machine learning-aided assessment of threats may incorrectly interpret regular exercises as acts of aggression and initiate excessive retaliation (Samaan, 2020).

Policy Gaps and Institutional Challenges

There is also a significant issue of the inexistence of detailed policy and regulatory structures in Pakistan that could be used to regulate AI and cyber defense. Although there are policies in the making, the realization efforts of such policies are still plagued by bureaucratic stagnation and technical shortage. According to Zaidi and Yusuf, (2023), unless there are separable doctrines on the use AI on the battlefield, Pakistan will stand danger of unchecked introduction of technologies that can be destabilizing.

In the literature, it is possible to see that the AI-enhanced cyberwar represents the key element of the U.S. and Chinese strategic competition, and it is important when discussing world security. Pakistan is a technologically weak but strategically crucial nation, and therefore has to cope with unique pressures of this digital battlefield. Its reliance on Chinese technology, limited indigenous AI capabilities, and exposure to regional cyber threats demand a comprehensive reassessment of its national security architecture. Future research and policy must focus on building resilient cyber infrastructure, investing in ethical AI frameworks, and promoting strategic autonomy in the digital domain.

Theoretical Framework

Offensive Realism as articulated by John Mearsheimer—asserts that the international system is fundamentally anarchic, meaning there is no overarching authority to enforce rules or guarantee the security of states9. In such an environment, states—especially great powers—are driven by an inherent desire to maximize their relative power and, if possible, achieve regional or global hegemony to ensure their survival9. For Mearsheimer, this pursuit of power is not a choice but a structural necessity9. In the context of your research, offensive realism provides a robust explanation for why the U.S. and China are locked in a relentless competition for dominance in AI-driven cyber warfare, and why this rivalry has profound implications for smaller states like Pakistan.

The U.S., as the established global hegemon, seeks to maintain its technological edge and prevent any challenger—most notably China—from eroding its dominance4. China, as a rising power, views its ascent as both inevitable and necessary for its survival and security, and thus aggressively pursues advancements in AI and cyber capabilities to offset U.S. advantages and assert its influence, particularly in the Indo-Pacific region4. This dynamic is not confined to conventional military spheres but extends deeply into cyberspace, where each side invests heavily in AI-driven offensive and defensive systems, conducts persistent cyber espionage, and seeks to disrupt or degrade the other's critical infrastructure8.

From an offensive realist perspective, the actions of both the U.S. and China are rational and predictable: each seeks to maximize its relative power to ensure its own security in a world where trust is scarce and conflict is always a possibility9. The rapid development and deployment of AI-enabled cyber weapons, autonomous systems, and advanced surveillance technologies are all consistent with the offensive realist expectation that states will exploit every available means to gain an advantage over rivals8. The lack of robust international norms or enforcement

mechanisms in cyberspace only heightens the incentives for states to act aggressively, as the risks of retaliation or punishment are often ambiguous or minimal4.

For a regional actor like Pakistan, offensive realism highlights the precarious position of smaller states caught between great power rivalries10. Pakistan's strategic calculus is shaped by the need to navigate the U.S.-China competition, seeking to leverage technological and military support from China while maintaining sufficient diplomatic flexibility to avoid over-dependence or provoking the U.S. and its allies. The May 2025 conflict with India demonstrated the risks and opportunities of this balancing act: Pakistan's reliance on Chinese AI and cyber support provided tactical advantages but also exposed vulnerabilities, as it remained susceptible to shifts in the broader U.S.-China relationship and potential pressure from either side10

Comparative Analysis: U.S. vs. China in AI-Driven Cyber Warfare

The strategic rivalry between the United States and China has entered a new phase with the rapid advancement of artificial intelligence (AI) and its integration into military and cyber operations. Both nations view AI as a critical enabler of future warfare, economic competitiveness, and geopolitical influence. This comparative analysis examines the contrasting approaches of the U.S. and China to AI-driven cyber warfare, focusing on their strategic doctrines, technological investments, operational methodologies, and the broader implications for global security and regional actors such as Pakistan.

The nature of AI-driven cyber warfare in the United States and China is rather different. The U.S. lays more emphasis on international partnerships, technological advantage, and incorporation of cyber power in the military activities, which also corresponds to the Third Offset Strategy. The 2023 Cyber Strategy released by the Department of Defense aims at the defense of the U.S. networks, countering the threats that are both great in magnitude and essential to the military and integrating cyber capabilities into military operations. The U.S. Cyber Command, since its foundation in 2009, has concentrated cyber operations and seeks to establish collaboration with the tech firms to capitalize on innovation.

The motive behind the cyber doctrine espoused by China is to gain the control of the region, and diminish the influence of the U.S. The People Liberation Army (PLA) combines AI in its intelligentized warfare policy, where there is the fusion of civilian and military innovation under the Military-Civil Fusion (MCF) policy. The Chinese way is centrally governed and state driven in terms of control over the cyber programs and legal demand on the level of adherence in the private sector.

The U.S model is based on the partnership of the people and the managerial innovation whereas the other is a centralized model with strict legal compliance to China wherein the private sectors are expected to comply. America focuses on transparency and resilience, whereas China has its vision defined by opacity and plausible deniability.

The U.S. is the global leader on the race of AI research and development, which is highly invested in by both the government and the industry. This is the AI roadmap deployed by the U.S. Cyber Command that involves about 100 tasks to integrate AI into logistics, security, and defense processes. Such initiatives as the Constellation project speed up the implementation of new AI activities. Quantum computing, autonomous systems and advanced form of encryption are also ventures that U.S. spends a lot of money on.

Implementation of the MCF policy and state investments have lead to China achieving great success in the field of AI, as well as cyber warfare. The PLA has also applied the AI to various offensive and defensive cyber use, automating the process of identifying and neutralizing threats and boosting information and psychological warfare abilities. China is utilizing its AI-enhanced cyber devices to monitor social media and other web-based interfaces to detect and defend disinformation runs, mold an opinion, and change the activities of enemies.

Also remarkable are improvements in quantum computing, hypersonics weapons, and swarm technology achieved by China. PLA is working on developing swarm drones with artificial intelligence that will perform intelligence and military deterrence. Huawei and other Chinese tech giants such as ZTE help improve cyber and AI capabilities of the nation and they tend to do so due to legal obligations to contribute to the state security actions.

The U.S. has an advantage in basic AI research and business innovation, and China is gaining even faster due to state-led investment and the MCF policy. Both countries are using AI in the surveillance of autonomous systems, cyber security and the intelligence sector, although the emphasis with China on swarm-tech and information warfare is unique.

The U.S and China are in a race to gain quantum supremacy since they have realized that it can disrupt encryption and beef up intelligence. Their operational styles of cyber warfare are marked with ambiguity, plausible deniability, and combination of cyber, information and psychological operations. Although the U.S. differs on its deterrence by relying on credible threats and alliances, China has its deterrence premised on ambiguity and the merging of cyber activities with the mass strategy.

The U.S. and China AI arms race is not an arms race alone in the 21st-century great-power politics and rivalries. Incorporation of AI in national security, economic plans and military interventions brings far-reaching challenges from strategic exposures and ethical problems to governance concerns.

The U.S.-China cyber competition opens up opportunities and threats that the regional players could take advantage of such as Pakistan which will have to manoeuvre amidst the competition; utilizing technological and military aid of the Chinese without relinquishing strategic diplomacy which may portray overdependence and antagonistic tendencies to the U.S. and other allies. This balancing act attracted the risks and opportunities as the tit-for-tat with India in May 2025 showed how Pakistani integration with Chinese AI and cyber capabilities gave it advantages in tactics but also took away its vulnerability. The development of national AI and cyber security capabilities in Pakistan plays the crucial role of ensuring strategic independence and resilience, in a more interfering digital environment.

International consequences: The AI race between the U.S and China is reshaping the balance of world powers, economic rivalry and technological dominance. Lack of international governance structures raises threat of escalation and unintentional results. Regional players such as Pakistan need to take the needed precaution that can prevent it being relegated or being bullied by emerging powers. Strategic autonomy and indigenous innovation are the key to understanding the complications of the digital battlefield.

both the U.S. and China have ethical, legal and governance issues. The U.S. promotes the concepts of "responsible AI" frameworks, and their development focuses on ethical aspects,

transparency, and safe, secure, and trusted AI development. Nonetheless, AI is highly prone to change and its dual-use character makes it hard to create good governance systems. The U.S has placed limits on exporting the advanced semiconductors and other strategic technologies to China, but the move poses a danger of limiting innovation and losing out on the international market to Chinese companies.

The Chinese used approach to AI governance is highly centralized and leaning toward national security being the main metric to consider rather than ethical considerations. Both the MCF policy and the National Intelligence Law keep an inkling that military applications are quickly exploited with the help of new developments in the progress made by the privately owned enterprises, disregarding moral and legal obligations in most cases. The opaqueness of China in AI science and technologic investigations increases suspicion and makes difficult the worldwide negotiation of principles and regulations on cyber warfare lodged on AI.

To a Pakistani, the solution out of the U.S.-China cyber race is to seek internal innovation, cybersecurity, and remain less reliant on foreign participants. To create a more robust and less dependent technological system in Pakistan, a greater investment in science and technology education, cooperation between all the economic sectors, and the establishment of international cooperation should be given priority. Pakistan also needs to come up with laws and ethical means of AI usage in defense, alleviate the threats that are posed by semi-autonomous systems and information warfare, and use AIs to pursue defensive and offensive operations in logic so as to sustain successful deterrence in the area.

Implications for Pakistan: U.S.-China AI-Driven Cyber Warfare and the Digital Battlefield

The increased rivalry between the US and China in the field of cyber war and artificial intelligence (AI) is the altering feature of how the world perceives security, particularly regional state such as Pakistan. The rivalry with India over the years, the significant role it plays in the global War on Terror and the complex relations it has with Afghanistan and China all impact on the strategic environment in Pakistan. This is a perilous situation complicated by the technology war between the U.S. and China. India-Pakistan clash, in May of 2025, revealed the payoffs and dangers of drawing down deeper strategic affiliations with China.

The reliance on China has not only improved the operations of Pakistan but also exposed it to alterations in the U.S.-China relationship in general due to reliance on China regarding defense technology like AI-driven systems. Such reliance is a bittersweet potion because it exposes Pakistan to the most advanced technology, but it also exposes Pakistan to the rather dangerous scenario that it becomes too much dependent on a single partner that may curtail its capabilities in decision-making during a crisis.

Things become fittingly difficult on the strategies of the Pakistani side by considering the fact that the technology ecosystems are fragmenting across and around the globe. The U.S. and its partners are imposing restrictions on Chinese tech firms and valuable supply chains. Such factor has the potential to put Pakistan under more pressure and weaker in implementing its own foreign policy.

Pakistan should plan to implement AI into its military and security systems since it will increase surveillance, intelligence, border and anti-terrorist activities by a significant margin. Lack of

trained labour, inadequate finances in technical training and research and development skills in the country on the other hand are keeping the technological advancement of Pakistan at bay.

The militarization of AI and the proliferation of skills in South Asian in terms of cyber war has massive security issues in Pakistan. The threats posed by India even diversify with the help of quick adaptation to AI-powered systems, which is assisted by the partnerships with the giant tech companies and the U.S. The placement of powerful cybersecurity systems and dedicated teams to safeguard AI-based infrastructure is no longer optional but necessary.

The outcomes of the U.S.-China tech competition impact Pakistani economy and development in a big way. The case of China which has been investing in the digital infrastructure in Pakistan is making the country to develop and modernize at a greater rate. The availability of 5G networks and AI-based systems has simplified the process of hooking to the internet, accelerated the digitalization process, and provided additional opportunities to innovate and create business. However, along with these changes, risks are involved, which include probable security threats, cyber attacks, and surveillance risks. The position of Pakistan on the map and lack of trust by people in its defense alliances with China make it more difficult to find investment and technological advancement of other countries to be availed to Pakistan.

The inclusion of AI to the national security system of Pakistan also raises vital policy and governance considerations, including a legal and ethical impact of militarizing AI. There is also the case of Pakistan, which has been at the forefront of promoting the regulation of militarization of the AI and even demanding that the world should ban autonomous weapon systems. This is however very difficult due to rapid changes in technology and powerlessness of domestic regulation systems. Pakistan must develop elaborate guidelines on how to develop, apply, and implement AI in the military and security. They should also involve clear policies of ethical governance, responsibility, and openness among the means to handle bias, privacy, and security threats.

There are numerous factors that are both wide and deep in terms of impacts of the US-China AI-driven cyber warfare race on Pakistan. The strategic issue faced by Pakistan is how it can modernize its military and retain its capability of remaining independent and avoid being dragged into the conflicts among the great powers. The nation must address the threats of digital addiction, digital security gaps, and deficiency of local productiveness technology-wise. The economic incentives are off set by the dangers of over-dependence on Chinese investments and the possible exclusion to the Western technological markets. In regards to this complex situation, Pakistan has to invest in developing national AI capabilities, enhancing its cybersecurity and a balanced and diverse foreign policy.

Conclusion

As the United States and China increasingly compete and engage in artificial intelligence (AI) and cyber warfare, it has immensely affected national security, economic evolution and geopolitical plans. The digital battlefield is not a theoretical concept anymore but it is an experience that has conditioned the boundaries of national security, economic progress, and geopolitical politics. Pakistan as it is located in the midst of great power competition and regional confrontation has great problems in coping with this fast changing world.

The U.S and China rivalry poses opportunities and risks to Pakistan. On the one hand, the strengthened strategic alliance with China has delivered to Pakistan highly developed military equipment, cyber vacuities, and important infrastructure investments, including the China-Pakistan Economic Corridor (CPEC) and the Digital Silk Road. These evolutions have improved the effectiveness of operations of Pakistan, growth in economy as well as modernization in technology. But this form of dependence on China has left Pakistan open to great vulnerability such as over dependence, control by an external source and ventilated into great power politics. The national security implication of AI-supported cyber warfare to Pakistan is multi-dimensional. The agile embrace of AI and cyber capabilities has increased the level of acts against Pakistan and a quick response, along with flexibility, is required. Emerging and developing social media intelligence (SOCMINT), highly data-driven, and autonomous system capabilities in Pakistan are heading towards the correct path, but important issues associated with them still exist. Limited resources coupled with the lack of well-funded technical education as well as a pool of skilled workers has prevented Pakistan not only to develop its own AI but also to enhance its cybersecurity infrastructure.

The fact that there is a risk of over-dependence and the threat of shutting off the market of the western technology equilibrium the Chinese investment benefits economically. To counter such risks, it is necessary that Pakistan focus on in-country development of its own AI capabilities and investing in education in science and technology and creating public-private partnerships to create a stronger, resilient self-reliant technology environment. It will need to diversify its technological importation and expertise sources to prevent over dependence on one partner and hence strategic flexibility in the world that is becoming highly polarized.

References

Allen, Gregory C., and Taniel Chan. “Artificial Intelligence and National Security.” Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2017.

Binnendijk, Anika, et al. “Autonomous Systems and the Escalation of Conflict.” RAND Corporation, 2021.

Brundage, Miles, et al. “The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.” arXiv, 20 Feb. 2018, arxiv.org/abs/1802.07228.

Creemers, Rogier, Paul Triolo, and Graham Webster. “China’s Strategic Thinking on Building Power in Cyberspace.” China Perspectives, no. 2, 2020, pp. 17–27.

Horowitz, Michael C., Paul Scharre, and Ben Garfinkel. “Artificial Intelligence and International Security.” International Security, vol. 45, no. 2, 2020, pp. 7–51.

Kania, Elsa B., and Lorand Laskai. “AI and National Security.” Center for Security and Emerging Technology, 2019.

Ng, Jason. “China’s Next Generation Artificial Intelligence Development Plan.” Asia Pacific Foundation of Canada, 2020.

Schaub, Gary, and Tim Maurer. “USCYBERCOM and the Integration of AI.” Survival, vol. 63, no. 2, 2021, pp. 123–144.

Singer, P. W., and Emerson T. Brooking. LikeWar: The Weaponization of Social Media. Houghton Mifflin Harcourt, 2018.

Bajaj, Simran, and Sameer Patil. “India’s Cyber Strategy and the China Challenge.” Observer Research Foundation, 2021.
Boulanin, Vincent, and Maaike Verbruggen. “Mapping the Development of Autonomy in Weapon Systems.” Stockholm International Peace Research Institute, Nov. 2017.
Clarke, Richard A., and Robert K. Knake. Cyber War: The Next Threat to National Security and What to Do About It. Ecco, 2010.
Gilli, Andrea, and Mauro Gilli. “Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage.” International Security, vol. 43, no. 3, 2018, pp. 141–189.
Hussain, Zahid, and Nida Ahmad. “Pakistan’s Cybersecurity Challenges in the Age of Digital Warfare.” Strategic Studies, vol. 42, no. 1, 2022, pp. 45–67.
Lin, Herbert S., and Amy Zegart, editors. Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations. Brookings Institution Press, 2019.
Mearsheimer, John J. The Tragedy of Great Power Politics. W.W. Norton & Company, 2001.
Suri, Gunjan, and Sanjib Choudhury. “India’s AI Ambitions and Regional Security.” ORF Issue Brief, no. 591, Observer Research Foundation, 2023.
Tang, Shaohua. “China’s Cyber Power in a Global Context: Strategic Ambitions and Policy Choices.” Journal of Strategic Studies, vol. 44, no. 5, 2021, pp. 750–772.
Taddeo, Mariarosaria, and Luciano Floridi. “Regulate Artificial Intelligence to Avert Cyber Arms Race.” Nature, vol. 556, no. 7701, 2018, pp. 296–298.
United Nations Institute for Disarmament Research (UNIDIR). “The Cyber Index: International Security Trends and Realities.” UNIDIR, 2020.