Journal of Regional Studies Review (JRSR)
Volume 4, Issue 1 (Winter 2025) | Pages: 424–432
ISSN (Online): 3006-6646
Digital Object Identifier (DOI): 10.62843/jrsr/2025.4a089
Correspondence should be addressed to Hafiza Ayesha Aslam; ayeshapakistani2001@gmail.com

RESEARCH ARTICLE

AI Driven Cyber Warfare Between China and India and Its Impact on Pakistan's National Security

Hafiza Ayesha Aslam [a]

Abstract: This study examines the evolutionary role of artificial intelligence (AI) in cyber war between China and India from 2020 to 2025 and its implications for the national security of Pakistan. With the two regional powers integrating AI in its cyber strategies - distributing disinformation campaigns to autonomous defense systems - the threat scenario in southern Asia has become increasingly complex. Pakistan, geologically situated between these rivals, faces unique vulnerabilities due to its underdeveloped cyber security infrastructure and AI limited resources. While China and India advance AI -oriented cyber operations, Pakistan remains exposed to digital espionage, AI -enhanced psychological operations and critical infrastructure attacks. This research explores the strategic response of Pakistan, including the formation of the Pakistan Computer Response Team (PKCERT), the development of a national cyber security authority, and the launch of its first IA policy by 2025. Study applies realistic and neorealist structures, emphasizing state competition, survival and relative power. The literature review identifies significant gaps, including the lack of triangular analysis between China, India and Pakistan, limited AI integration into the national defense of Pakistan and the regional cyber security cooperation. The article concludes with political recommendations to improve Pakistan AI and cyber resilience, emphasizing the construction of domestic capacity, legal reforms and strategic alliances to ensure national security in the digital age.

Keywords: Artificial Intelligence, Cyberwar, Warfare, India, Digital Age, China, Cyber Security, Pakistan, Impact of Cyberwarfare

Introduction

Cyber war refers to the use of digital attack using space, noted that this war is more dangerous than war with weapons. This is when group countries use the internet to attack each other, the most powerful intrinsic weapon. Cyber war is an attack on the system of others, which is unauthorized access, stealing data and use for its own benefit. Cyber war and cyber terrorism are quite similar; only the difference is level. Crime that is committed to international data in the form of data, digital attack, spying, sabotage, manipulation, political tactics and military objectives, etc. This is the advanced form of terrorism and attack, by cyber-attack a country damage the dorsal spine of the other country and without dorsal spine how can one survive or remain correctly? Cyber War is actually attacks by state sponsors of non -state actors, including hackers, criminals and agencies. The main agenda includes lies scattered to cause chaos, spread wrong information and misinformation. Every country needs a strong cyber security system to protect itself from the attack. The purpose of the striker's County is to attack the political and economic of other municipalities, weaken his military, military, to harm his public interest and attack his unity and peace. India and China, they are not only having border dispute, but they also have cyber war by which they are fighting with the internet and technology instead of weapons and soldiers. in the context of China (Khalid 2025). Next, some of the hacked Indians in the history of hackers by China Tibetan -related sites in India. China has placed the harmful

[a] Student, Department of Political Science and International Relations, University of Management and Technology, Lahore, Punjab, Pakistan.

Cite this Article: Aslam, H. A. (2025). AI Driven Cyber Warfare Between China and India and Its Impact on Pakistan's National Security. *Journal of Regional Studies Review, 4*(1), 424-432. https://doi.org/10.62843/jrsr/2025.4a089

software (malware) on these websites to spy on the Indian who visit them, spyware to watch people who talk against the Chinese government, including those of India.

According to Microsoft, China can use (artificial intelligence) to publicize false news to confuse people and influence public opinion. In the context of India, they do not openly admit that they are attacking China's couch but are working and overthrowing their cyber security institute and training their hackers. Alao countries such as the US, Japan and Israel help Indian hackers to train them hardly and at the top, for their own purpose, and weaken their mutual enemies. India strengthens its defense institutions as a reaction. I.E, Drdo cyber research program, cooperation with allies, CERT and its cyber agency for defense. Hackers can easily or silently enter. Obviously, there is always a law of action and reaction. Every country is strengthening its defense and research institutions as a protective shield against any cyber-attack. Every country did not attack others openly or by an announcement, there is a hidden strategy. Both countries are better in their cyber system and strategy, it would be dangerous to increase. In any kind of war, this not only affects these two countries, but it is also a threat to the neighboring country and enemies or confidant of both countries, especially those who have weak cyber defense system. Pakistan is directly affected in this cyber war between China and India, unfortunately Pakistan neither has a single cyber security company. Pakistan is a municipality of 23 crore of the population and about 18 million intelligent phones are actively using in a country. Pakistan does not have a single application. They buy apps and block their phones that are easily accessible and hacked by hackers. What insecure purchases Pakistan has. How Pakistan and India have no good relationships; On the other hand, China is confidant of Pakistan.

India is doing active attacks on Pakistan too. action and Reaction are a main role here. Both the countries spread false news by attacking their softwares. mainly India Spreads hate and target the unity of country by using Pakistan Identity through internet. Their aint fail is their agenda by attacking Pakistan with bomb and weapons through source of cyber-attack.

AI Is Changing Cyber Warfare

Artificial intelligence is a program that can think, learn and make decisions nearly like humans. AI helps a lot specially in Cyber Attacks, Smarter not harder work phenomenon applies. AI helps in Smarter hacking through which Hacker can identify the weak spot in websites and networks faster Changing malware, it is a software that is bad in nature. AI can easily change itself by getting protect and cannot be detect by any virus. AI is using is Phising, can generate very professional and look real emails that can easily use to hack someone and access to their passwords and links.

Per Contra AI as a reaction feels friendly, AI can detect hacking activities easily and block hackers automatically. AI can make fake videos or voices that look very real, it spread lies. AI can use specially during war, no doubt AI defends better but yes, it is a fact that AI is a new threat, and the deadly relation of AI and Cyber terrorism is perilous. Pakistan held very important position in south Asia, located between two rivals India and China (Ibrahim 2024).

India is using its Digital India program to boost its technology power, working with global tech companies to become a cyber leader. China is using big projects like the Belt and Road Initiative (BRI) and the Cyber Silk Road to grow its influence around the world, including in cyberspace. Pakistan is caught in the middle of the growing cyber conflict between India and China. While it maintains a close relationship with China through projects like the China-Pakistan Economic Corridor (CPEC), which strengthens its position against India, Pakistan's weak cyber defenses and heavy reliance on foreign technology make it vulnerable. To stay secure and avoid being drawn into the India-China cyber rivalry, Pakistan must focus on building strong cybersecurity, developing its own technology, and forming partnerships with other nations. Balancing international cooperation with self-reliance is essential for Pakistan to protect its interests and maintain.

There is changing cyber war: Artificial intelligence is a program that can think, learn, and make almost human beings. AI helps a lot, especially in cyber-attacks, applies the smartest phenomenon of work. AI helps smarter hackers, through which the hacker can identify the weakness on faster malware sites and networks, is software that is bad by nature. AI can easily change yourself, obtaining protection and cannot be detected by any viruses. AI is using it is phising, can generate very professional and look for and emails that can easily use to invade someone and accept their passwords and links. Contrary, as a reaction, AI can easily detect hacker activities and block hackers automatically. AI can make fake videos or voices that look very real, it spread. AI can use especially during the war, none DIUBT defends itself better, but rather, it is a fact that AI is a new threat, and the deadly rehabilitation of AI and cyber terrorism is dangerous. Pakistan occupied a very important position in southern Asia, located between two rivals in India and China. India is using its India digital program to increase its technological power, working with global technology companies to become a cyber leader. China is using major projects such as Belt and Road Initiative (BRI) and Cyber Silk Road to increase its influence around the world, including cyberspace. Pakistan is caught in the midst of the growing cyber conflict between India and China. Although it maintains a close relationship with China through projects such as the China-Pakistan Economic Corridor (CPEC), which strengthens its position against India, the poor cyber defenses of Pakistan, and the strong dependence on foreign technology make it vulnerable. To remain safe and avoid being attracted to the Indian cyber rivalry,

Research Questions

1. How has AI been used in cyber warfare between China and India, Implications for Pakistan's national security in South Asia? (2020-2025)
2. How can Pakistan strengthen its cyber and AI capabilities to maintain national security (2022-2025).

Theoretical Framework

The most suitable theory is Realism (Thomas Hobbes), According to Realism States act realistically to protect self-interest and gain power, protect dignity and sovereignty. In this Research Both the States want to influence each other and limit other's power. Also, theres is a concept of Relative Gains. There's also crux find with Neorealism that is structural realism by Kenneth Waltz which says that the structure of international system (anarchy) forces states to compete and naim goal is to gain power and control.

Problem Statement:

With the rapid integration of artificial intelligence (AI) into modern military and cyber capabilities, the escalating cyber warfare competition between China and India poses significant challenges to regional stability. As both nations invest heavily in AI-driven cyber operations—ranging from espionage and surveillance to offensive cyber capabilities—Pakistan finds itself in a vulnerable position. The geopolitical tension and technological arms race increase the risk of cyber spillover effects, strategic miscalculations, and digital disruptions that could compromise Pakistan's national security infrastructure, including critical information systems, defense networks, and economic sectors. This research seeks to analyze the implications of the AI-powered cyber conflict between China and India on Pakistan's national security, while identifying strategic gaps and proposing frameworks for cyber defense resilience.

Literature Review:

In South Asia, the induction of AI into cyberspace has critically altered the security environment. As big regional powers, China and India have put AI use to boost their cyber capabilities, resulting in intricate geopolitical dynamics. For Pakistan, the location between these two countries means that it stands to take advantage of the strategic merits and pitfalls that come with the proliferation of AI-powered cyber warfare. This paper is a literature review of the AI in cyber warfare and its consequences for Pakistan's national defence.

AI in Cyber Warfare: A Global Perspective

In the age of AI, the nature of cyber warfare has changed, and AI has provided nations with the means to execute highly advanced cyber operations at speeds and scales the world has never seen before. AI helps to automate the attacks on the cyberspace, improve the threat detection mechanism, and even adapts to the defence. Yet the double-edged nature of AI technology also represents considerable peril, including no small risk of escalation and the erosion of the distinctions between cyber and kinetic warfare. Academics have claimed that the fast pace at which AI is developing within the cyber domain calls for a new era of international cyber norms and arms control.

China's AI-Driven Cyber Capabilities

China has been leading the way in incorporating AI into its cyber plans. Some reports suggest Chinese state-supported actors have used AI to carry out influence operations: these activities have involved deploying AI-generated content to derail elections and stoke dissension in places like Asia and the US. These actions typically include utilizing deepfake technology with mass automated bots to amplify propaganda and disinformation. Furthermore, the priority given to AI by China for military use is contributing to advances in autonomy in use of force and cyber capabilities, raising questions about what consequences that may have for regional security stability.

India's AI-Enhanced Cyber Warfare Initiatives

India has also been aggressively working to include AI in its cyber warfare systems. Setting up of the Defence Artificial Intelligence Project Agency (DAIPA) will showcase India's seriousness in developing AI enabled battle systems such as drones or unmanned vehicles, next gen cyber capabilities etc. Besides, India's NCCC (National Cyber Coordination Centre) is an important agency in the detection and prevention of cyber threats, but controversies related to surveillance and privacy have been raised. Artificial Intelligence in India's Defense Artificial Intelligence in India's Defense Artificial Intelligence (AI) permeation of India's defense system has strategic ramifications for its relations with other countries, especially Pakistan.

Pakistan's Cybersecurity Landscape and AI Integration

Pakistan's cybersecurity framework has evolved in response to the growing threats in the cyber domain. The establishment of the Pakistan Computer Emergency Response Team (PKCERT) in 2024 marked a significant step toward enhancing the nation's cyber resilience. Additionally, initiatives like the Presidential Initiative for Artificial Intelligence and Computing (PIAIC) aim to promote AI education and research, potentially fostering advancements in AI applications for national security. However, challenges persist, including limited indigenous AI capabilities and the need for robust cybersecurity policies to counter evolving threats. (Pakistan Computer Emergency Response Team).

Implications

The proliferation of AI in cyber warfare by neighboring countries presents multifaceted challenges for Pakistan's national security. Potential threats include cyber espionage targeting critical infrastructure, disinformation campaigns aimed at destabilizing societal cohesion, and the risk of miscalculations leading to escalatory cycles. Moreover, the integration of AI into military strategies by China and India could alter the regional balance of power, compelling Pakistan to reassess its defense and deterrence strategies. Scholars emphasize the importance of developing a comprehensive national cybersecurity strategy that incorporates AI capabilities to safeguard Pakistan's interests (Hussain 2025).

The intersection of AI and cyber warfare is reshaping the security landscape in South Asia. For Pakistan, understanding the AI-driven cyber strategies of neighboring countries is crucial for formulating effective defense policies. While AI offers opportunities for enhancing cybersecurity and defense capabilities,

it also introduces new risks that require careful management. Future research should focus on developing frameworks for regional cooperation in cybersecurity, establishing norms for responsible AI use in military applications, and enhancing Pakistan's indigenous AI capabilities to ensure national security in the evolving digital age.

Literature Gap

As Artificial Intelligence (AI) rapidly transforms the nature of cyber warfare and strategic security paradigms globally, the South Asian region is witnessing an evolving techno-strategic competition, particularly between China and India. While literature has emerged analyzing these developments in bilateral and global contexts, a significant gap remains in understanding the *triangular implications* for Pakistan. This literature gap highlights areas where academic inquiry is lacking and underscores the necessity for focused research to assess the implications of AI-driven cyber warfare on Pakistan's national security.

Lack of Integrated Triangular Analysis (China–India–Pakistan)

Much of the existing research tends to focus on China's or India's cyber and AI military capabilities independently, or in the context of bilateral tensions with the United States or the West. For example, numerous studies explore China's digital influence operations, AI-enhanced surveillance state, and offensive cyber capabilities targeting Taiwan, the US, or its internal dissidents. Similarly, India's cyber capabilities are often studied through the lens of its national cybersecurity policy or its response to cyber threats emanating from China.

However, there is a marked absence of studies that simultaneously examine China and India's AI-driven cyber strategies through the lens of their strategic impact on Pakistan Pakistan, which shares complex historical, geopolitical, and security ties with both neighbors, remains largely underrepresented in the current scholarly debate surrounding AI-enabled cyber threats and regional military-technological competition.
In particular, there is insufficient analysis of how the escalation of AI-powered cyber capabilities by China and India might pressure Pakistan to adapt or retaliate, either technologically or diplomatically. This triangular dynamic—central to South Asia's balance of power—has yet to be thoroughly explored in academic or policy literature.

Minimal Exploration of AI Integration in Pakistan's National Security Framework

Another major gap in the literature is the lack of detailed study on Pakistan's integration of AI into its cyber defense and national security strategies**. While official initiatives like the Presidential Initiative for Artificial Intelligence and Computing (PIAIC) and the creation of Pakistan's Computer Emergency Response Team (PKCERT) have been launched, academic engagement with these developments is sparse (Hira Bashir 2024). There is very limited scholarly research analyzing the effectiveness and limitations of these initiatives.

The Actual Deployment of AI tools in Pakistan's Cyber Defense Systems

The institutional readiness of Pakistan's military and civilian agencies to adapt AI for cybersecurity and cyber warfare.

Comparative analysis of Pakistan's AI capabilities vis-à-vis India and China

Moreover, while AI research in Pakistan is growing in the academic sector, there remains a disconnect between technological innovation and strategic military application, a gap that needs thorough investigation.

Understudied Role of AI-Powered Disinformation in Regional Conflicts

A particularly critical gap in the literature is the under-examination of AI-enhanced disinformation campaigns and their role in regional conflict escalation. Emerging global literature has begun to examine

how AI is used to manipulate public opinion, influence elections, and destabilize societies through tools such as deepfakes, automated troll farms, and bot-generated propaganda.

China has been accused of leveraging AI tools to conduct influence operations globally, while India has similarly been implicated in digital misinformation campaigns, particularly during sensitive political events or conflicts. However, the specific use of AI in shaping perceptions, narratives, and psychological operations (PSYOPS) during India–Pakistan or China–Pakistan standoffs is largely missing from academic and policy analysis.

This gap is significant, as AI-driven information warfare could become a tool for indirect aggression between these nuclear-armed states. Understanding the potential of disinformation to trigger misperceptions, civilian unrest, or even military escalation is crucial for crafting effective national security strategies.

Absence of Pakistan-Specific Cybersecurity Frameworks in AI Context

Though international think tanks such as RAND, Carnegie Endowment, and Chatham House have published frameworks for responsible AI use in military and cyber contexts, there is little effort to adapt these frameworks to the unique geopolitical, technological, and security realities of Pakistan (Ghani 2025).
Pakistan faces a distinct set of challenges:

- Infrastructural underdevelopment in digital domains.
- Limited indigenous AI research funding and implementation capacity.
- Regional isolation in terms of cyber cooperation.
- Proximity to two technologically superior adversaries.

Despite this, few studies have attempted to propose or evaluate cybersecurity doctrines that incorporate AI for defensive or strategic use in the Pakistani context. There is a need for research that explores how Pakistan can:

- Build indigenous AI capabilities.
- Enhance cyber deterrence and resilience.
- Cooperate regionally to avoid conflict escalation.

Lack of Research on Regional Cyber Confidence-Building Measures (CBMs)

The academic literature also lacks exploration of cyber diplomacy or cyber confidence-building measures (CBMs) between China, India, and Pakistan. While nuclear CBMs have been studied in depth, their cyber equivalents are still underdeveloped. Given the high potential for accidental escalation due to misattributed cyber-attacks or AI errors, this is a major oversight.

Unlike NATO or the European Union, South Asia has no institutionalized cyber norms or AI-related military agreements. The potential of AI to amplify cyber incidents, interfere with early-warning systems, or disrupt command and control structures raises the risk of rapid conflict escalation in the region. Research into multilateral or trilateral agreements on AI and cyber norms, especially involving Pakistan, is urgently needed (Khan A. M., 2025).

Scarcity of Empirical Data and Case Studies from the Region

Finally, there is a general lack of empirical data, regional case studies, and incident-specific analysis that link AI-enabled cyber operations to security outcomes in South Asia. While the global North benefits from advanced tracking of cyber incidents, attribution methods, and public reporting, cyber warfare events in South Asia often go unreported or are heavily politicized, limiting academic engagement.

Few peer-reviewed studies document real-world cyber incidents involving AI tools in India-Pakistan or China-Pakistan relations. This lack of transparency and data availability hampers evidence-based analysis and policy formulation.

To summarize, the existing literature on AI-driven cyber warfare is rich in global perspectives but insufficiently tailored to the strategic, technological, and political realities of South Asia, particularly regarding Pakistan. There is an urgent need for academic and policy research that:

- Explores the triangular cyber dynamics between China, India, and Pakistan.
- Assesses Pakistan's preparedness to face AI-enabled cyber threats.
- Investigates the role of AI in regional disinformation and PSYOPS
- Develops context-specific frameworks for Pakistan's cyber defense.

Promotes regional cooperation on AI and cyber norms to prevent conflict escalation. Filling these gaps will not only enhance scholarly understanding but also contribute to more robust and resilient national security strategies for Pakistan in the face of rapidly advancing AI-driven threats.

Research Questions

1. How has AI been used in cyber warfare between China and India, and what are the implications for Pakistan's national security in South Asia (2020–2025)?
2. 2.How can Pakistan strengthen its cyber and AI capabilities to maintain national security (2022–2025)?

1. AI in Cyber Warfare Between China and India: Implications for Pakistan's National Security (2020–2025)

The integration of Artificial Intelligence (AI) into cyber warfare strategies has significantly altered the security dynamics in South Asia. Both China and India have increasingly employed AI to enhance their cyber capabilities, leading to complex geopolitical challenges for neighboring countries, particularly Pakistan.

China's AI-Driven Cyber Capabilities

China has made the most out of AI in its cyber strategies. In English-speaking democracies, Chinese state-sponsored actors are using AI to influence elections and foment discord From Asia to the U.S., governments are using AI models to create fake content to disrupt elections and fuel dissent. These operations frequently rely upon deepfake techniques and automated bots to disseminate propaganda and disinformation. Furthermore, China's prioritization of AI in military applications has driven progress in autonomous systems and cyber capabilities, causing anxiety over what that means for regional security stability.

India's AI-Enhanced Cyber Warfare Initiatives

India, too, has done reasonably well in using AI in the cyber warfare plans. The creation of the Defence Artificial Intelligence Project Agency (DAIPA) highlights India's determination to develop military AI, including on unmanned platforms and cyber. The provision of funds is meant to counter the rising trends of cyber-crime and in a functioning for the country's own National Cyber Coordination Centre (NCCC) which has met with opposition as the center was designated for surveillance and has raised privacy concerns." The use of AI in Indian defence installations also has an impact on the strategic posture and its relations with its antagonistic neighbour Pakistan.

Implications for Pakistan's National Security

Neighboring countries use AI for cyber warfare, which poses many dimensions of threat to national security of Pakistan. Possible threats range from cyber espionage of critical infrastructure to disinformation campaigns meant to break up societal unity to the danger of miscalculation and escalation in crisis situations. Also, the use of AI in military doctrines of both China and India can potentially change the regional

power equations, requiring Pakistan to revise their defense and deterrence postures. The academia has also pointed out the need for a holistic national cyber security policy with incorporation of AI adeptness for the protection of Pakistan's interests. Boosting Pakistan's Cyber and AI Capabilities for National Security (2022-2025) In view of cyber threats that continue to emerge, Pakistan has taken some steps to enhance its cyber security and AI capabilities.

Formation of National Cyber Security Authority

Pakistan to establish National Cyber Security Authority by 2025 in what is described as significant move towards securing its cyberspace. They will oversee organizations' use of security-validated infrastructure, the new power will ensure data breaches and cyberattacks are thwarted. This initiative will fill the gap between the public and private sectors and encourage public private partnerships in the sphere of cyber security in Pakistan.

Development of AI Policy

The government will announce its first Artificial Intelligence (AI) Policy in early 2025. The policy is designed to enhance cyber security with comprehensive facilities to identify and develop countermeasures for cyber threats in real time, thus preventing data breaches. The policy also aims to lift digital economy and make the country a "Digital Pakistan." The creation of this policy draws on the cooperation of industry, academia, the private sector, and the government and emphasizes the need for a broad and effective policy formulating process.

Establishment of Pakistan Computer Emergency Response Team (PKCERT)

Pakistan introduced Pakistan Computer Emergency Response Team (PKCERT) in March 2024 to tackle emerging threats in form of cyber threats and hacking attacks against different public sector organisations. It is PKCERT that is responsible for cooperation in dealing with cybersecurity incidents and threats and improving the country's ability to handle cyber events. "Setting up PKCERT is an important milestone on Pakistan's path towards stronger cyber-security and resilience (Ahmad 2022).

Strategic Recommendations for Strengthening Cybersecurity

While on the security front, Pakistan needs to take some strategic steps to fortify its cyber borders, which include defeating the use of law not only for warfare but as instrument of lawfare against Pakistan and updating laws to fight fake news and digital impersonation, especially with the increase in use of artificial intelligence. The tension between freedom and privacy needs answers, and mandatory government and civil employee cybersecurity education must be considered. Furthermore, a National Cyber Security Agency would consolidate monitoring, and crisis communication plans need to be made to repair public trust after cyber incidents. Building robust threat-sharing mechanisms and fostering partnerships around the globe are also critical to improving cyber preparedness.

Conclusion

Incorporating AI in the cyber warfare doctrine of neighboring countries adds on to the ordeal of national security in Pakistan. In reaction, Pakistan has launched a series of initiatives to enhancing its cybersecurity and AI capabilities. Ongoing work to develop and execute holistic cybersecurity approaches and promote cooperation between stakeholders is necessary to protect Pakistan's digital base and national security against dynamic cyber threats.

References

Ahmad, A. (2022). *Navigating cybersecurity cooperation between China and Pakistan.* Paradigm Shift. https://www.paradigmshift.com.pk/cybersecurity-pakistan-china/

Artificial Intelligence led Lethal Autonomous Weapon Systems and Terrorism: Risk Assessment and Solutions for Pakistan. *CISS Insight Journal, 12*(1), 24-55. https://journal.ciss.org.pk/index.php/ciss-insight/article/view/361

Bashir, H., Zarish, W., & Malik, R. (2024). The role of AI in hybrid warfare: A case study of Pakistan's cybersecurity landscape. *Global Strategic & Security Studies Review, 9*(1), 86–93. https://doi.org/10.31703/gsssr.2024(IX-I).08

Farid, A., & Sarwar, G. (2024). Artificial Intelligence and National Security: Future Warfare Implications for Pakistan. *Annals of Human and Social Sciences, 5*(2), 446–459.https://doi.org/10.35484/ahss.2024(5-II-S)42

Farid, A., & Sarwar, G. (2024). Artificial intelligence and national security: Future warfare implications for Pakistan. *Annals of Human and Social Sciences, 5*(2), 446–459. https://doi.org/10.35484/ahss.2024(5-II-S)42

Ghani, M. U. (2025). US-China cyber security warfare: Implications on Pakistan (2018–2024). *Social Sciences & Humanity Research Review, 3*(1), 40–60. Retrieved from https://jssr.online/index.php/4/article/view/57

Hussain, Y., & Khan, D. (2025). *South Asia's AI arms race*. Center for International Strategic Studies (CISS) Pakistan. https://ciss.org.pk/south-asias-ai-arms-race

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

Khan, A. M., & Khan, A. A. (2025). Cyber-deterrence and cyber-CBMs: Way forward for managing India-Pakistan cyber rivalry. *Journal of Asian and African Studies*. https://doi.org/10.1177/00219096251332932