Journal of Social Sciences Research & Policy (JSSRP)

GISSR
Global Institute of Social Sciences Research

Impact of China's Cyber Security Role on South Asia and Neighboring Countries

Khush Bakht
MPhil Scholar, Department of Political Science, Abdul Wali Khan University Mardan, Pakistan.

How to Cite This Article: Bakht, K. (2025). Impact of China's Cyber Security Role on South Asia and Neighboring Countries. *Journal of Social Sciences Research & Policy. 3 (03), 494-503.*
DOI: https://doi.org/10.71327/jssrp.33.494.503

ISSN: 3006-6557 (Online)
ISSN: 3006-6549 (Print)

Vol. 3, **No.** 3 (2025)
Pages: 494-503

Key Words:

China, Cyber Diplomacy, Pakistan, South Asia, Digital Sovereignty

Corresponding Author:
Khush Bakht
Email: khandurani483@gmail.com

Abstract: *This study examines the expanding role of China in shaping South Asia's cyber landscape, with particular focus on its growing digital partnership with Pakistan. As China strengthens its cyber diplomacy through initiatives such as the Cyber security Law, the cyber-sovereignty doctrine, and the Digital Silk Road, its influence increasingly extends into the technological infrastructures and cyber security frameworks of neighboring states. The literature reveals that China–Pakistan cyber cooperation has moved beyond traditional military and economic ties, creating new dynamics in regional power relations, digital sovereignty, and security governance. While Pakistan aligns closely with Chinese cyber norms, other South Asian countries, such as India, Bangladesh, Sri Lanka, and Nepal, struggle to balance the economic benefits of Chinese digital investments with concerns about surveillance, data control, and strategic dependence. The study identifies major cyber security vulnerabilities across South Asia, worsened by limited institutional capacity and weak legal frameworks, underscoring the need for stronger regional collaboration. It concludes that China's cyber engagement is reshaping regional geopolitics and highlights the urgency for South Asian states to develop coordinated cyber security strategies to safeguard their digital autonomy and maintain stability in an increasingly contested cyber domain.*

Introduction

The rapid development of the internet and digital technologies in the 21st century has created new opportunities and challenges in international relations, security, and diplomacy. Cyber diplomacy, which refers to the use of diplomatic methods in the digital space to manage international relations, has become a crucial element in the foreign policy strategies of numerous states. As one of the world's most technologically advanced nations, China has emerged as a leading player in the domain of cyber diplomacy. Its increasing engagement in digital affairs is closely tied to its broader geopolitical strategy, including its deepening relationship with Pakistan.

The phenomenon of globalization has modeled every aspect of human life, mainly seen as the compression of time and space at the grand strategic level. International relations among the states have also been shaped by this phenomenon in the information age and reliance on technologically driven diplomatic practices is growing leading to newly explored dimensions of diplomacy (Munir, Mahmood & Malik, 2023). Various factors create stress on national governments to remodel their foreign policy structures for the development of mass engagements as the focus of their political and diplomatic outreach. These factors include enhanced cultural exchanges, media explosions, plurality of populace, interdependence, and enhanced globalization (Barrinha & Renard, 2017).

A transition has therefore been observed from traditional diplomacy to cyber diplomacy to compete for rapidly paced strategic engagements and management of international affairs. The plethora of social media platforms and escalated use of computer networks have given an impetus for realizing the true potential of digital diplomacy. The diplomatic as well as technological competence for the application of these tools is thus required to acquire desired outcomes (Alawida, Omolara, Abiodun & Al-Rajab, 2022).

In the rapidly evolving digital age cyber diplomacy has become a pivotal element in the strategic calculations of global powers. China in particular has emerged as a significant player in the cyber domain leveraging its technology and development initiators to shape global cyber government. One of the critical areas where China has focused its cyber diplomacy in South Asia with Pakistan as a key strategic partner, The Sino-Pakistani alliance traditionally rooted in military and economic cooperation, has increasingly extended into the cyber realm rising important questions about regional cyber security digital sovereignty and Geo political stability (Ball, Béraud-Sudreau, Huxley, Raja Mohan & Taylor, 2019).

This research seeks to examine China's cyber diplomacy in the context of its partnership with Pakistan focusing on how this relationship influences regional cyber governance, frameworks and broader geo political dynamics. China revealed that there were seven incidents attributed to the Indian hackers group "Bittter"in 2022 and eight attacks in 2023,targetting China and Pakistan. China ranked 3rd at threat level. In defensive measures Chinese President Xi Jingping adopted a cyber-diplomacy. While there is considerable literature on China's cyber strategies and Pakistan's role within the belt and road initiative (BRI), specific cyber dimensions of this partnership remain underexplored. This study aims to fill this gap by analyzing the strategic motivation behind China's cyber diplomacy with Pakistan and assessing its implications for both regional and global cyber governance.

Problem Statement

The cyber partnership between China and Pakistan represents a significant shift in South Asia's power dynamics moving beyond traditional military and economic ties to focus on cyber security. This growing relationship raises important questions about regional security, digital sovereignty and the impact on global cyber governance, however there is a lack of detailed research on how China cyber environment with Pakistan affects these areas. This study aims to address this gap by exploring the influence of this partnership on Pakistan digital sovereignty and the broader security landscape in South Asia

Research Objective

- To examine the impact of Sino-Pakistani cyber collaboration all regional balance of powers.

Overview of China’s Growing Cyber Influence

The Chinese nation has transformed into a global leader regarding cybersecurity systems. China utilizes its cyber influence aspirations to reach global leadership through digital space dominance which enables national interest protection under developed technological capabilities.

China’s Cybersecurity Strategy

The cybersecurity strategy across China underwent considerable development during recent times following the implementation of the Cybersecurity Law of the People's Republic of China in 2017. China created this law as its digital sovereignty package which established guidelines to ensure data protection along with domestic internet control (China Law Translate, 2017). Data localization requirements together with domestic auditing duties under this legislation prevent foreign businesses from operating smoothly while building up Chinese digital authority. Through legal means the Chinese government acquires the authorization to monitor online actions while upholding national security interests based on Creemers (2017) analysis.

The international cyber diplomacy initiatives by China pursue aggressive standards for promoting Chinese regulations worldwide. The cyber sovereignty initiative is a main aspect of China's international cyber diplomacy campaign since it claims that every nation holds the right to manage their digital and internet infrastructure independently from outside intervention. Global actors have adopted the principle of cyber sovereignty from China and cooperated with it during UN and WTO diplomatic engagements (Zeng, 2020).

China’s Role in Global Cyber Governance

China plays an active role in international efforts to mold the emerging standards of cyber governance across the world. The UN Group of Governmental Experts on Cybersecurity (GGE) functions as an international organization where China contributes proposals focusing on its state-oriented digital governance goals (Bennet, 2019). The Belt and Road Initiative (BRI) of China has succeeded in achieving partnerships with numerous nations from Africa through Asia until Latin America to support their cybersecurity development and adoption of Chinese technologies with Huawei central to constructing telecom systems.

By engaging in alliances China presses its technological authority alongside cybersecurity control into partner countries which enables it to dictate digital policies. Chinese firms implemented the development of 5G networks and cyber security services in Sri Lanka which has raised questions about Chinese control over essential national infrastructure (Murphy, 2020).

Technological Dominance and Export of Cybersecurity Solutions

The global expansion of firms including Huawei, ZTE and Alibaba has bestowed China with unmatched power to expand its digital infrastructure across the world. The network infrastructure and cybersecurity solution offering through these companies has resulted in their entry into multiple South Asian countries including Pakistan alongside Bangladesh and Sri Lanka as per Ramanathan (2020). Chinese collaborations with these countries offer economic advantages and cyber surveillance strength which enables China to modify national security frameworks in these areas.

The South Asian region observes an increasing partnership between Huawei and local operators for 5G network deployment. The 5G network rollouts in Pakistan heavily involve Huawei but simultaneously raise concerns about Chinese access to country-sensitive data networks (Subramanian 2020). The increasing usage of Chinese tech companies has led numerous nations particularly India and Bangladesh to develop concerns regarding both cyber intelligence gathering and digital national sovereignty and data protection.

The Digital Silk Road

China utilizes the Digital Silk Road platform as its main digital influence project under the Belt and Road Initiative (BRI). According to Zeng (2020) the Digital Silk Road functions as a digital infrastructure building program across Asia Africa and Europe in order to establish China's position as the world leader of information and communication technology (ICT). The governments of Pakistan along with Sri Lanka and Nepal have received heavy investments from China for digital infrastructure development which extends into Chinese cybersecurity tools and surveillance capabilities within their technology solutions.

China built a smart city under the BRI in Sri Lanka through installation of its technology which provides the possibility for Chinese government control over Sri Lankan digital infrastructure (Murphy 2020). Such developments challenge nations to determine what level of security should exist between infrastructure growth and foreign control of vital database communications.

Cybersecurity and Economic Leverage

China extends its cyber influence through economic leverage which operates beyond technological and infrastructure-based elements. The BRI framework allows China to become essential global ally to many countries across South Asia because China provides technology solutions and financial loans at affordable costs. These partnerships create major political as well as cybersecurity threats (Rahman, 2018). Countries that depend heavily on Chinese technology systems become exposed to security risks because this technological relationship could force them to follow Beijing's digital policy goals at the expense of their country's independence.

The Bangladesh public faces surveillance concerns because their national telecom infrastructure depends on Chinese technology from Huawei companies. Multiple security reports suggest these technology companies maintain unauthorized entry to communication networks that could serve as tools for espionage and intelligence collection (Ramanathan, 2020).

China’s Cybersecurity Strategy and Objectives

China implements a rapidly developing cybersecurity strategic framework that serves its national security interests across the nation. China's framework for cybersecurity contains the Cybersecurity Law of the People's Republic of China which started operating nationally in 2017. Through its national legislation China Law Translate (2017) established goals to bolster security measures while securing their digital sovereignty and defending internet-based rights of citizens. China achieves digital control domestically and worldwide through its hard restrictions on online content along with its requirement for keeping data within local boundaries (Creemers, 2017).

Cybersecurity Challenges in South Asia

The countries within South Asia including India, Pakistan, Bangladesh, Sri Lanka, Nepal, Bhutan and Afghanistan encounter substantial cybersecurity risks that block their capability to protect national priorities alongside critical infrastructure and digital independence. Regional cybersecurity challenges intensify because of political competitions throughout the area combined with advanced electronic attack techniques and slow progress in creating multinational cyber defense plans.

Vulnerabilities in South Asia

The process of digitalization has brought significant advances for South Asian countries in the face of severe deficiencies in their cybersecurity infrastructure. These challenges become more difficult because South Asian governments lack adequate cybersecurity laws and frameworks and their countries do not have enough trained security professionals. A World Economic Forum (2020) report indicates that South Asian nations occupy rankings among the lowest in worldwide cybersecurity assessments because their populations show poor cybersecurity knowledge while having insufficient data protection laws and weak security policy implementation standards.

One of the world's biggest economies alongside its position as the second-largest internet user base has not solved India's cybersecurity threats adequately. Despite progress from National Cyber Security Policy (2013) and Indian Computer Emergency Response Team (CERT-In) in improving cybersecurity the nation's quick technological expansion now exceeds its ability to create sufficient security standards (Ramanathan, 2020). The countries of China and Pakistan frequently target India with state-sponsored cyberattacks for purposes of espionage and espionage-related operations (Subramanian, 2020).

Multiple breaches of critical systems occur in Pakistan because the country faces issues with weak regulatory frameworks alongside insufficient national infrastructure cybersecurity and the absence of a unified cybersecurity strategy. Cybersecurity Ventures (2021) released a report showing that Pakistan experienced major cyberattacks that could have been politically motivated against government websites and security agency digital platforms (Rahman, 2018).

Need for Regional Cooperation

The rising digital connections between South Asian nations coupled with escalating transnational cyber hazards require these states to join forces in cybersecurity matters. SAARC possesses the ability to become a vital organization that performs information sharing and conducts joint cybersecurity drills while building capability development programs. The CERT-In initiative from India shows how regional organizations can share information yet the region requires more investments to establish defensive cyber architecture against both national and non-national threats (Ramanathan 2020).

The vulnerability of South Asia's critical infrastructure will decrease when the grassroots levels of smaller nations develop their core cybersecurity awareness and capacity. Enhanced cyber education together with training programs represent the key solution to address digital security management barriers facing the region because of its severe cybersecurity skills gap (Zeng, 2020).

China’s Influence on International Cyber Norms and South Asia’s Position

China pursues international cyber norm influence by advocating state regulations of cyberspace in order to achieve its national objectives. The Chinese government utilizes its Cybersecurity Law of the People's Republic of China (2017) to implement cybersecurity standards that enforce state-governed internet management and extensive digital information regulations as outlined by Subramanian (2020). China uses its advocacy for state-controlled cyber governance to lead international cybersecurity dialogues at United Nations and BRICS since these organizations work under its cyber sovereignty framework.

South Asian nations must make difficult choices between Western internet liberation principles and Chinese cyber sovereignty demands as Beijing applies intense pressure on them to create policies that satisfy Chinese political objectives. Indian opposition stands against Chinese cyber regulations but Sri Lanka together with Bangladesh confront an increasingly difficult situation due to China's expanding economic power which enables control over digital policies (Zeng, 2020). The China-Pakistan Economic Corridor functions as a tool for forming digital interdependence because Pakistan has begun to implement its cybersecurity policies according to Chinese standards (Rahman, 2018). South Asian digital sovereignty faces an increasing threat from Chinese influence because different nations integrate Chinese technologies into their operations.

Strategic Implications for South Asia: Digital Sovereignty and Regional Cooperation

The expanding Chinese influence over cyber policy creation in South Asia establishes fundamental strategic effects. Regional collaboration between countries becomes essential because China pursues cyber sovereignty initiatives. The free internet and unrestricted information flow backed by India concerns this nation about how Chinese digital operations affect their network activities. The Indian cybersecurity approach centers on maintaining digital independence while enhancing national cybersecurity systems as protection against rising threats from Chinese technological products (Ramanathan, 2020).

Small Asian countries such as Sri Lanka along with Nepal and Bangladesh struggle to manage Chinese infrastructure agreements because they need to safeguard both their cyber security and digital independence. A collaborative regional cybersecurity program could effectively stop China from controlling cyber space throughout the region. South Asian Association for Regional Cooperation (SAARC) needs to initiate a regional cybersecurity framework that fights rising cyber threats through mutual support and data exchanges about cybersecurity (Murphy, 2020).

India is working through the Quad framework alongside the United States and Japan and Australia to confront Chinese cyber dominance in the area as per Subramanian (2020). The partnerships aim to create stronger online defenses while promoting free internet standards which push back against Chinese internet control practices.

Conclusion

The reviewed literature demonstrates that China's expanding cyber capabilities and its deepening digital partnership with Pakistan is reshaping South Asia's strategic landscape. China's cyber diplomacy, rooted in its Cybersecurity Law, cyber-sovereignty principle, and Digital Silk Road, extends its technological, economic, and political influence across the region. Through infrastructure investments, cybersecurity solutions, and the export of surveillance-capable technologies, China strengthens its leverage while raising concerns about data security and digital dependence among South Asian states. Pakistan, as China's closest regional partner, experiences the strongest alignment with Chinese cyber norms, contributing to a shifting balance of power that challenges India and impacts regional cyber governance. Meanwhile, states such as Sri Lanka, Nepal, and Bangladesh face difficult decisions as they balance the benefits of Chinese digital investments against risks to sovereignty.

Overall, the literature highlights a growing need for coordinated regional cyber frameworks, stronger domestic cybersecurity capacities, and multilateral collaborations, such as the Quad to counterbalance China's influence. As South Asia becomes increasingly interconnected and vulnerable to cyber threats, the China–Pakistan cyber partnership stands as a pivotal factor shaping digital security, strategic alignments, and the future of cyber governance in the region.

References

Adams, J. (2021). NATO's Cyber Defense Pledge: Progress and Challenges. *Journal of Cybersecurity Policy, 14(2)*, 67-89.

Ahmed, N. (2021). Cybersecurity in South Asia: The role of China and Pakistan in shaping the future of cyber defense. Asian Security, 17(3), 299-315. https://doi.org/10.1080/14799855.2021.1893456

Ahmed, R. (2023). "The Geopolitics of Space: Pakistan's Space Program in the Context of Global Rivalries." Asian Strategic Review.

Ahmed, S. (2018). Cyber Security in South Asia: A Study of Pakistan and China's Digital Strategies. Islamabad: National Defence University Press.

Ahmed, T., & Zhao, L. (2022). Cybersecurity in South Asia: China-Pakistan Digital Cooperation. *Asian Journal of International Affairs, 14*(2), 201-220.

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences, 34(10),* 8176–8206.

Alden, C. (2017). China's Cybersecurity Strategy: Implications for Global Politics. *Journal of International Relations and Development.*

Alden, E. (2017). China's Comprehensive National Power and Cyberspace Strategies*.* China Security Review*, 5(2),* 33-56.

Alden, E. (2017). China's Digital Silk Road: Expanding its Influence through Cyberspace. *Journal of International Relations and Cybersecurity, 9(3),* 52-74.

Amin, R. (2020). China-Pakistan Economic Corridor: An analysis of the economic impact on Pakistan. *Journal of Asian Economics, 68, 15-27*. https://doi.org/10.1016/j.asieco.2019.12.005

Ashraf, S. (2015). China Pakistan Economic Corridor. *Institute of South Asian Studies, 364(9),* 1–4. https://doi.org/10.2139/ssrn.2608927

Assoudeh, M. (2020). Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative

Perspective (Doctoral dissertation, University of Nevada, Reno).

Banerjee, A. (2023). Cybersecurity Challenges in South Asia. *Cyber Defense Journal, 12(3),* 45-67.

Banks, W. C. (2016). Cyber espionage and electronic surveillance: Beyond the media coverage. Emory LJ, 66, 513.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. Global Affairs, 3(4-5), 353–364.

Bennet, R. (2019). China's Digital Silk Road: What it means for cybersecurity. *International Journal of Cyber Policy, 12(3)*, 45-61.

Benson, R. (2021). Cyber Terrorism: A Growing Threat. International Security Review, 18(3), 34-56.

Berg, M. (2018). Cyber Diplomacy in the 21st Century: A New Approach to Global Security*. International Journal of Cyber Security and Digital Diplomacy, 5(2),* 47-59.

Briggs, R. (2019). The Digital Silk Road: China's Expanding Role in Global Infrastructure*. Journal of Asian Infrastructure and Development, 22(4),* 1-15.

Buchan, R., & Navarrete, I. (2021). Cyber espionage and international law. In Research handbook on international law and cyberspace (pp. 231-252). Edward Elgar Publishing.

Buffaloe, D. L. (2006). Defining asymmetric warfare. Arlington, VA: Institute of Land Warfare, Association of the United States Army.

Cai, C. (2015). Cybersecurity in the Chinese context: changing concepts, vital interests, and prospects for cooperation. China Quarterly of International Strategic Studies, 1(03), 471-496.

Cave, D. (2017). The Internet and the Future of Global Governance: China's View on Cyber Sovereignty*. China Quarterly, 223,* 209-225.

Chaudhry, F. (2021). Digital Diplomacy and Cybersecurity Challenges in South Asia. *South Asian Studies, 17*(3), 145-167.

Chen, X. (2021). Digital sovereignty in the age of cyber diplomacy: The China-Pakistan nexus. *Asian Journal of International Affairs, 14(3),* 67-89.

Chen, Y. (2023). Quantum Computing and Cybersecurity: Future Challenges. *Journal of Emerging Technologies, 29(1),* 78-91.

Clarke, R. (2010). *Cyber Warfare: A Beginner's Guide*. Oxford: Oneworld Publications.

Clarke, R. (2021). State-Sponsored Cyber Activities: Implications for National Security. *Cyber Defense Journal, 12(3)*, 45-67.

Creemers, R. (2017). China's Cyber Diplomacy: A Strategy for Global Influence. *Journal of Contemporary China, 26*(105), 673-689.

Creemers, R. (2017). China's Cybersecurity Law: Implications for internet governance and Chinese sovereignty. Global Policy, 8(4), 425-439.

Creemers, R. (2017). China's vision for cyber sovereignty. *Georgetown Journal of International Affairs, 18(3)*, 28-36.

Cunningham, D. (2018). *China's Cyber Diplomacy: The Interplay of Economic and National Security*. Pacific Review, 31(2), 225-246.

Cybersecurity Ventures. (2021). Cybercrime in Pakistan: Trends and Statistics. Cybersecurity Ventures. https://www.cybersecurityventures.com

Das, R. (2023). Indigenous Cyber Technologies and National Security. Indian Technology Review, 29(2), 78-91.

Dawn. (2021). *The early years of Sino-Pakistani relations*. Dawn. Retrieved from https://www.dawn.com/news/1557599

Deibert, R. (2008). Control and Censorship: The Future of Cyber Diplomacy*. Journal of International Affairs, 62(1)*, 89-104.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. Global Governance, 18, 339.

DeNardis, L. (2014). The Global War for Internet Governance. Yale University Press.

Greene, M. (2021). Pakistan's Cyber Dilemma: Balancing China and the West. *Strategic Cyber Review, 9*(1), 55-70.

Gul, A. (2022). Sino-Pakistani cyber collaboration: Regional cyber governance and security implications. *South Asian Journal of Policy and Governance, 12(2),* 89- 102.

Gul, F., & Jamil, M. (2021). Cybersecurity cooperation between China and Pakistan: Strategic dimensions and implications*. Journal of Strategic Security, 14(2),* 91-110. https://doi.org/10.1080/19434047.2021.1901591

Gupta, P. (2021). Cyber Warfare and Its Geopolitical Implications. *International Journal of Cyber Studies, 10(1),* 33-50.

Huang, Y. (2020). The Military Dimensions of China's Cyber Strategy. Strategic Studies Quarterly, 14(3), 45-67.

Huang, Y. (2020). The Military-Civil Fusion and China's Cybersecurity Strategy. *Journal of Cybersecurity Strategy, 12(3)*, 45-67.

Hughes, B. (2023). Global Cybersecurity Norms and Regulations*. International Journal of Cyber Policy, 9(1),* 67-89.

Hunt, M. H., & Westad, O. A. (1990). The Chinese Communist Party and International Affairs: A Field Report on New Historical Sources and Old Research Problems. The China Quarterly, 122, 258-272.

Johnson, M. (2023). Strengthening Public-Private Partnerships in Cybersecurity. Cybersecurity & Policy Review, 22(3), 56-74.

Johnson-Freese, J. (2016). Space warfare in the 21st century: Arming the heavens. Routledge. Moltz, J. C. (2019). The politics of space security: Strategic restraint and the pursuit of national interests. Stanford University Press.

Joshi, M. (2021). China-Pakistan Cyber Collaboration: An Emerging Threat to India. Strategic Studies Quarterly, 15(4), 22-40.

Joshi, R. (2022). India's Response to China-Pakistan Cyber Collaboration. *Indian Journal of Strategic Studies, 11*(3), 78-95.

Kanwal, S., Pitafi, A. H., Ahmad, M., Khan, N. A., Ali, S. M., & Surahio, M. K. (2020). Cross-border analysis of China– Pakistan Economic Corridor development project and local residence quality of life. *Journal of Public Affairs*.

Khan, M., & Rana, A. (2021). Cyber cooperation between China and Pakistan: Implications for cybersecurity in South Asia*. International Journal of Cybersecurity and Digital Governance, 4(1),* 33-45.

Khan, S. (2021). Digital Trade and E-Commerce: China's Expanding Role in Pakistan's Cyber Economy. *International Journal of Digital Commerce, 15*(4), 98-115.

Khan, S. (2022). "The Militarization of Space and the Strategic Implications for South Asia*." Journal of International Security.*

Kim, T. (2023). AI in Cybersecurity: Opportunities and Risks. *Journal of AI and Cyber Studies, 15(2)*, 90-110.

Klein, J. (2020). The Hidden Risks of China's Cyber Diplomacy. *Global Cybersecurity Review, 7*(2), 67-80.

Kshetri, N. (2019). China's cyber security strategy and its impact on South Asia.

Kumar, S. (2023). India’s Cybersecurity Strategy: Countering Threats from China and Pakistan. *Journal of Strategic Affairs, 18(3)*, 56-73.

Li, Z. (2017). *The Role of Cyber Diplomacy in China’s Foreign Policy*. Asian Studies Review, 41(4), 1-15.

Liang, F., & Xue, L. (2019). Cyber warfare and the Chinese military: The evolution of China’s cyber defense capabilities. *Journal of Strategic Studies*, 42(4), 434-456. https://doi.org/10.1080/01402390.2019.1673190

Lindsay, J. R. (2014). The impact of China on cybersecurity: Fiction and friction. International Security, 39(3), 7-47.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.). (2015). China and cybersecurity: Espionage, strategy, and politics in the digital domain. Oxford University Press.

Liu, J. (2020). *China’s cyber diplomacy: A case study of Sino-Pak cooperation in cybersecurity*. *Journal of International Relations, 48(2),* 214-230. https://doi.org/10.1080/01402390.2020.1795645

Mahmood, A. (2021). *The role of Chinese technology firms in Pakistan’s digital transformation*. *Asian Technology Journal, 22(3)*, 45-60. https://doi.org/10.1016/j.astech.2021.01.003

Mahmood, S. (2019). Cyber diplomacy: A case study of Sino-Pak cooperation. *Journal of International Relations and Development, 22(2),* 174-190. https://doi.org/10.1057/s41311-019-00092-9

Mehta, V. (2022). National Cyber Defense Mechanisms in India. Defense Technology Review, 14(1), 67-84.

Mishra, D. (2019*).* Cyber Collaboration and National Security in South Asia: China and Pakistan’s Partnership*. Asian Journal of Security Studies, 13(2),* 35-52.

Müller, K. (2022). The EU Cybersecurity Act: Implications and Future Directions. *European Cyber Journal, 11(3),* 45-62.

Patel, D. (2021). Disinformation Warfare in the Digital Age. Journal of Cyber Intelligence, 7(2), 90-110.

Patel, S. (2020). Cyber Terrorism and Digital Radicalization. Journal of Security Studies, 17(1), 33-50.

Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. Faber & Faber.

Qureshi, Z., & Jan, M. (2020). Strategic Cyber Collaboration Between China and Pakistan: A Review of Security Dimensions*. Journal of South Asian Politics, 18(3)*, 245-263.

Rahman, M. (2018). Economic implications of China’s cybersecurity influence in South Asia. *Journal of International Trade and Development, 25(4*), 678-693.

Ramanathan, A. (2020). Huawei and China's strategic influence in South Asia's telecom infrastructure. South Asian Review, 12(2), 88-101.

Ramanathan, A. (2020). Huawei and China's strategic influence in South Asia's telecom infrastructure. South Asian Review, 12(2), 88-101.

Rana, M. (2021). China-Pakistan Economic Corridor (CPEC) and its impact on digital infrastructure. *South Asian Journal of Technology, 29(4)*, 439-455. https://doi.org/10.1080/07288451.2021.1794560

Rana, S. (2020). The Pakistan-China Fiber Optic Project: Strategic Implications. *Telecommunications Review, 6*(2), 134-152.

Rao, T. (2020). China and Pakistan’s cybersecurity collaboration: An evolving partnership. *South Asian Journal of Cybersecurity*, 8(1), 57-71. https://doi.org/10.1007/s13405-020-0025-x

Raza, S. (2020). Cyber Sovereignty and Pakistan: The Impact of China’s Digital Influence*. Asian Journal of International Relations, 6(1),* 29-45.

Raza, S., & Ali, M. (2021). Digital Silk Road: China-Pakistan technological cooperation and future prospects*. Journal of International Trade and Technology, 18(4)*, 121-134. https://doi.org/10.1080/23455729.2021.1868741

Rehman, M. (2020). China-Pakistan: A Technological Partnership in the Age of Cyber Diplomacy. *Asian Journal of Political Science, 15(3),* 79-92.

Segal, A. (2018). China's Vision for Global Cyber Governance. *Council on Foreign Relations Report, 1*(3), 15-29.

Segal, A. (2020). China's alternative cyber governance regime. Council on Foreign Relations, 1-8.

Shackelford, S. (2015). Cybersecurity and International Relations: Challenges for China. Asian Politics and Policy, 7(4), 489-509.

Shah, A. (2015). Pakistan's military cooperation with China: An evolving partnership*. Asian Affairs, 46(3),* 472-488. https://doi.org/10.1080/03068374.2015.1055036

Shah, S. (2019). The China-Pakistan Cyber Relationship: Implications for Global Digital Governance*. Digital Asia, 23(1),* 49-62.

Zhao, J. (2017*).* Pakistan and China: A strategic alliance in the post-Cold War era*. South Asian Studies Review, 14(2),* 205-220. https://doi.org/10.1080/15384910.2017.1360712

Zhao, L., & Khan, A. (2021). The geopolitical dimensions of Sino-Pak cyber security cooperation*. International Affairs, 98(3),* 741-756. https://doi.org/10.1093/ia/iiab055

Zhao, Y. (2015). China's Internet Diplomacy: An Emerging Model*. Asian Security Studies Journal, 6(2),* 115-132.

Zhao, Y. (2020). China's Digital Silk Road and Its Impact on Global Internet Governance*. Global Policy, 11(4),* 305-312

Zhou, Y., & Li, C. (2019). China's Belt and Road Initiative and Cyber Expansion. *International Relations Journal, 20*(1), 34-50.

Zubair, S., & Ghosh, A. (2017). CPEC and Cyber Infrastructure in Pakistan: Chinese Investments and Geopolitical Implications*. Pakistan International Affairs Journal, 45(4),* 212-230.