JRSR
JOURNAL OF REGIONAL STUDIES REVIEW

Journal of Regional Studies Review (JRSR)
Volume 4, Issue 1 (Winter 2025) | Pages: 414–423
ISSN (Online): 3006-6646
Digital Object Identifier (DOI): 10.62843/jrsr/2025.4a088
Correspondence should be addressed to Aleena Sadi; aleenasadi49@gmail.com

RESEARCH ARTICLE

U.S.-China AI Rivalry and its Implications on Pakistan's Cybersecurity and Digital Sovereignty

Aleena Sadi [a]

Abstract: This paper examines the implications of the US-China AI rivalry on Pakistan's digital sovereignty and national security through the lens of offensive realism. Pakistan, sandwiched between its strategic cooperation with China and historical links with the United States, has increasing cyber risks, technology dependence, and autonomous concerns. The paper, which draws on primary data from Pakistani cybersecurity institutions, case studies from similarly situated countries, and significant policy documents, demonstrates how the USA and China cyber race exacerbates these challenges. With 78% of its vital digital infrastructure relying on Chinese technology and little domestic skills, Pakistan is still vulnerable to cyber-espionage, data breaches, and future geopolitical coercion. The article emphasises that such dependence could compromise national security, especially as systemic pressures rise. The paper provides the comprehensive policy recommendations to improve resilience and foster indigenous digital capabilities. Additionally, it promotes regional cyber collaboration, relationship diversification, and technology non-alignment.

Keywords: U.S.-China AI Rivalry, Pakistan Digital Sovereignty, Cybersecurity Infrastructure, China-Pakistan Economic Corridor (CPEC), South Asian Cybersecurity, Technological Dependence, Defensive Realism

Introduction

Artificial intelligence (AI) has become the focus of great power competition in the twenty-first century, making geopolitics like nothing seen before. Former Pentagon strategist Robert Work writes, The AI competition between Washington and Beijing will prove more consequential for international order than the nuclear arms race of the Cold War era. The contest swirling between China and the US is very different from that in the past, being a high-tech, borderless, interconnected race where civilian and military uses of AI merge and affect millions instantaneously. AI systems are deciding everything from what we read online to how particular threats are monitored by governments (Buchanan, 2022). Yet behind this innovation is an underlying contest for influence and dominance a technology arms race between the U.S. and China that is slowly rewiring the foundation of global power. It is not your typical geopolitical battle. It is a strategic struggle for the early 21st century that will shape the balance of economic power, the configuration of global digital governance, and the national security arrangements among the states (Yildirim, 2025). For other emerging economies, Pakistan in particular, this competition is not a faraway question of strategy on which academics debate, but an urgent national challenge, one that directly affects the country's digital infrastructure, national security, and ultimate sovereignty over the long term. The options that Pakistan opts for today to traverse its technological inversion will reverberate for decades; either taking off as an independent digital actor or continuously chaining itself to external technological appendages.

Although this competition is decades old, China's emergence as a global AI force was turbo-charged in the early 2000s. China was once the world's workshop and has become a high-tech powerhouse, primarily through state-backed initiatives, such as the 863 Program, the “Made in China 2025" plan, and the 2017

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

Cite this Article: Sadi, A. (2025). U.S.-China AI Rivalry and its Implications on Pakistan's Cybersecurity and Digital Sovereignty. *Journal of Regional Studies Review, 4*(1), 414-423. https://doi.org/10.62843/jrsr/2025.4a088

publication of its key Next Generation Artificial Intelligence Development Plan, which gamed out how China was going to take over the world (and was specifically challenged to do so in AI by 2030) .Since then, China has scaled AI from facial recognition for mass surveillance and predictive policing to smart cities, autonomous weapons systems, and smart infrastructure across sectors and borders at a dizzying pace. Not only has Beijing fused these technologies into its society, but it has also done so with ruthless intent to propagate the project to the developing world, often packaged up with its sprawling architecture of physical infrastructure under the Belt and Road Initiative (BRI). Pakistan has been one of the main beneficiaries and even the natural strategic partner in this technology push (Sacks, 2022). Meanwhile, the other end of this rivalry, the U.S., long considered the world leader in innovation, is now engaged in strategic reassessment. Washington is no longer complacent, as it once was, about Chinese technological growth. The United States, for its part, has responded with various measures from export controls on key technologies to sanctions on Chinese tech firms like Huawei and ZTE, and major legislation in the form of the recently passed CHIPS and Science Act that seeks to revitalise local semiconductor manufacturing and Chinese tech competition. Beyond economic metrics, this competition has taken on an ideological character. The U.S. advocates a democratic digital governance model that is more decentralised, more privacy-minded, and market-oriented. Alternatively, China promotes an integrated digital environment that is under state control, where technology advances development objectives and political control alike (Ali, 2020).

That ideological split, which some analysts are now referring to as the "bifurcation of the global tech ecosystem", has driven a wedge into the digital world as the space fractures into two competing spheres of influence. With these contending models intertwined with geopolitics, countries, particularly in the Global South, are being put on the spot to pick a side. The implications for Pakistan are especially severe, given that the digital advancement of the country is closely linked to both superpowers (Javed, 2021). However, the country's historic security and aid-based ties with the U.S. create strategic contradictions and competing pressures in technology governance, even as its strategic alliance with China has quickened modernisation through digital infrastructure projects, cloud computing services, and surveillance networks chiefly dominated by firms such as Huawei. Such a double dependency opens up scope for accelerated digital transformation, as well as large-scale vulnerabilities. In 2023, China accounts for nearly 78% of the critical digital infrastructure of Pakistan (Pakistan Telecommunication Authority, 2023). Though the technologies came as a means to increase connectivity, surveillance, and urban management, they have also led to deep-rooted data sovereignty, cybersecurity, and the risk of foreign surveillance and control concerns. The growing digitisation of defence, financial, and energy networks in Pakistan is increasingly exposing them to geopolitical risk. Lacking sufficient local capabilities in AI development, encryption, or hardware manufacturing, Pakistan is charting a course through a future in which technological dependency may slowly undermine its strategic autonomy (Dong, 2025).

The US-China technological rivalry, too, raises some questions for the regulatory frameworks and data governance regimes of Pakistan. As the threats of espionage, cyberwarfare, and disinformation campaigns grow, the state is struggling to find a way to protect its citizens' data, provide secure channels for digital communication, and order the digital domain independently. Simultaneously, the international pressure to gravitate towards either one or the other digital superpower is likely to politicise the technology policy choices of Pakistan and force it into binary choices which may not be in its national interest (Khan, 2022).

Research Questions

This paper aims to further examine these dynamics through an inquiry building on two primary research questions:

1. What Impact Does US-China AI Rivalry Have on Cyber Security Empowerment and Digital Sovereignty of Pakistan?

2. How can Pakistan prevent becoming completely dependent on technology while keeping a balanced relationship with both digital superpowers?

In order to address these questions, this article utilizes primary data through institutions in Pakistan like the National Response Center for Cyber Crimes, case studies with similar digitally developing states and theoretical underpinnings through international relations. In Pakistan, for example, advanced cyberattacks have increased by 18% each year since much of this is directed towards government databases and financial infrastructure (NR3C, 2023). These attacks amplify the need for secure and sovereign digital ecosystems. We are faced with an elder face of obstacles, and the future is not etched in stone. This window is still open for Pakistan by strategically diversifying technology partners, investing in local digital capacity-building, as well as formulating strong cybersecurity and data protection legislation. Pakistan can choose between a digitally sovereign state and a restructured dependence on a singular technological force. The technological road that Pakistan chooses to ride today will dictate its path towards tomorrow in terms of choice to adopt, ally and invest in the required infrastructure for the inevitable digitalisation that is upon us. In the end, Pakistan is at an inflexion point. As moves towards a techno-community continue across the globe and where advances in technology increasingly dictate national strength and stature, the choices Pakistan makes in its journey will not only seek to solidify Pakistan's place in the order of the future but could also be defining of Pakistan's aspirations in the areas of sovereignty, security and self-determination through technology in the current information century.

Theoretical Framework

Practically, it is rather difficult to assess the negative effects of the US-China AI rivalry on Pakistan's digital infrastructure and cybersecurity without taking a step back and inspect through the lens of a theory; in this case the theoretical framework of defensive realism which is grounded in the work of Kenneth Waltz and has been elaborated further by Stephen Walt r at the theoretical level and applied level. The basic premise of defensive realism is that the international system is anarchic, there is no overarching authority, and states face struggles for survival by adopting prudent, security-maximising behaviours, meaning that they do not seek expansion of their power beyond what is necessary to achieve security. Such outlooks not only explain Pakistan's precarious position while grappling with the technological competition of two superpowers, but each one also trying to be the hegemon in the AI domain by sabotaging the interests of the other.

The US-China AI competition is a textbook security dilemma event: the very dynamic that defensive realism is built on. With both countries pouring immense sums into AI-enabled weapons systems, cyber capabilities, and digital infrastructure, and their steps to secure national security leading them to unintended responses through the security dilemma, the situation is one where tensions cannot help but rise & systemic instability is solely but a function of the sheer weight of power colliding into one another (Khan, 2022). This dynamic is particularly pressing for Pakistan. Its dependence on Chinese technology as one of the partners in the China-Pakistan Economic Corridor (CPEC), Huawei's 5G networks and surveillance systems, has invited the US' scrutiny on the ground that these dependencies are just part of Beijing's long-term strategy. As a result, Pakistan is punished with curbs like limited access to Western technologies, such as US sanctions under the Clean Network Initiative. At the same time, linkage with Chinese infrastructure makes it vulnerable to state-sponsored cyberattacks, especially from India, which has recently stepped up cyberespionage campaigns against Pakistani institutions. Defensive realism explains how Pakistan's efforts to protect its digital development, by a 'marriage with China', have on the contrary, increased Pakistan's susceptibility to external threats.

Additionally, the defensive features of realism and its focus on strategic restraint and the avoidance of overextension provide important lessons for Pakistan regarding how it should approach cybersecurity. Defensive realism is a much more nuanced theory compared to that of offensive realism, which underpins

the quest for power maximisation and entails measures for secondary states like Pakistan based on acquiring "sufficient" security, relying on the promotion of home-grown capacity development and de-escalation of entrapment into great power rivalry. The technological dependencies of Pakistan today, however, reflect a strategic imbalance: almost 80 per cent of its critical digital infrastructure is dependent on China, while the country faces losses because of a cybersecurity regime that fails to match sophistication with sophistication. This excessive dependency on outside actors is antithetical to the defensive realist notion that states need a degree of autonomy in a self-help system. The theory would comply with some kind of diversified strategy with less unilateral dependencies, investments in national AI and encryption technologies, and alignment with neutral states (e.g. South Korea or the EU) to escape coercion from the US or China. The idea of defensive posturing, another core principle of defensive realism, would at the same time further shape the options that Pakistan has in terms of cybersecurity policy. As such, amidst an age of AI-driven cyber war supplemented by autonomous malware, AI-enhanced Doxxing and the ubiquitous threat of state-sponsored hacking, Pakistan needs to proactively prioritise defensive manoeuvres instead of adopting a myopic view of Indian attribution vis-a-vis its offensive capabilities. This entails the institution of strong data localisation laws to stop foreign spying, the roll-out of quantum-resistant encryption to protect national communications, and the deployment of AI-powered automated threat detection systems to find and eliminate cyber-attacks in real-time (Javed, 2021). These messages are in keeping with defensive realism's prescription that states focus on securing their sovereignty rather than entering zero-sum technology races.

Lastly, defensive realism emphasises the value of institutional endurance and strategic foresight over decades. The low state of cybersecurity in Pakistan, as evident from its low position in global indices and frequent attacks on critical infrastructure, manifests a lack of securitisation of digital governance. Its doctrine would advance a coordinated national approach, inserting cybersecurity as an inescapable core component of national security, aligning military, economic, and diplomatic activities to decrease risk. That requires not just modernising technical defences but also developing personnel, reforming educational programs to churn out AI experts, and participating in the forums where international norms around the governance of new technologies will be determined. Therefore, defensive realism offers a nuanced explanation for Pakistan's challenges as symptoms of systemic pressures arising out of an anarchic international system, including factors relevant to cybersecurity. By integrating the principles of the theory of strategic moderation, defensive positioning, and institutional resilience, Pakistan can optimally exploit the changing dynamics of technological competition by minimising risks as well as having the internet within its digital sovereignty. The other option, unbridled reliance on one or another superpower, would make Pakistan a pawn on the digital chessboard of the Cold War, stripping the country of autonomy and jeopardising national security in a world where AI is not likely to become less relevant.

The US-China AI Rivalry: Structural Dimensions

The competition in the high-tech domains of military innovation, economic infrastructure, and cybersecurity between the US and China has important ramifications for Pakistan's national security, digital sovereignty, and its long-term growth. Washington and Beijing are rushing to incorporate artificial intelligence into their military infrastructure. The United States has established the Joint Artificial Intelligence Centre (JAIC), toral AI capabilities ranging from autonomous weapon systems, predictive logistics, to battlefield data integration (Dong, 2025)In a parallel move, China has recently established something called the Strategic Support Force within the People's Liberation Army (PLA),placing a strong focus on information warfare and command at machine speed powered by artificial intelligence (Sarfaraz, 2025). This AI-induced militarisation presents a multi-layered security dilemma for Pakistan. Counterintuitively, the domestic incorporation of Chinese statistical surveillance technologies and facial recognition systems strengthens internal counterterrorism capacities and border security. However, greater dependence on these systems could spark regional responses scrutiny from Western allies and fears of domestic surveillance and data privacy violations.

Nowhere is the economic angle of the US-China AI competition more obvious than in terms of investments in digital infrastructure. China's Digital Silk Road initiative, an outgrowth of the Belt and Road Initiative, has digitally connected more than 138 countries (Sacks, 2022) Thanks to the China-Pakistan Economic Corridor (CPEC), Pakistan has become an important hub of this growing ecosystem of technology. But along with the perks of such a partnership come strategic vulnerabilities. Debt liabilities related to CPEC have been rising to almost $4.9 billion, in words of (State Bank of Pakistan, 2023) and Need for Dependency or debt. Additionally, Pakistan's telecom infrastructure is highly dependent on Chinese technology, with 92% of the network operated through companies like Huawei and ZTE (Authority, 2023), leading to a lock-in effect of such technology. Although inexpensive, these systems have come under international scrutiny; several potential backdoors and surveillance risks in Chinese-produced devices were highlighted in Symantec's 2022 cybersecurity report. This is a threat not just to national security. It would also dilute Pakistan's negotiating leverage with other partners.

The CPEC Digital Ecosystem

Pakistan's augmentation of digital enmeshment with China is most visible in the China-Pakistan Economic Corridor (CPEC), which, from an infrastructure-focused modality, is morphing into a key digital domain. A quick technographic analysis showcases a strong presence of Chinese technologies in critical domains (Ali, 2020).Meanwhile, the role of Huawei in the expansion of Pakistan's 4G and 5G market cannot be overstated, with coverage reaching over 70 per cent of urban sites in 2023. Similarly, has supplied monitoring systems in several safe city initiatives in Islamabad and Lahore, including facial recognition and license plate reading technologies. More recently, ministries and other institutions of the government have used Alibaba Cloud for the storage and processing of data. While citizen data flows through and gets processed by systems they have limited insight or control over, raising important questions on data sovereignty (Authority, 2023). The trend of reliance is further proven in the startup ecosystem as of now, according to a research report, while more than 60 per cent of AI and cloud-based Pakistani startups utilize Chinese development frameworks of Paddle Paddle, their American-based counterparts, on the other hand, use TensorFlow or AWS (Pakistan, 2021). Additionally, lots of maintenance and support system contracts are with Chinese vendors, which makes an independent cyber response unlikely from Pakistan. These figures reflect structural dependency linked to the defensive realist fear of diminished sovereignty as much as economic entanglement. It revealed multiple vulnerabilities within CPEC-linked digital infrastructure, including port logistics platforms in Gwadar that employ AI-enabled scheduling and inventory systems, as was not disclosed in full by the 2023 National Infosec Audit (Azhar, 2024) Experts flagged issues including unencrypted data transmissions and insufficient audit trails, which could expose the controls to cyber-espionage or even hijacking by external third parties. Such empirical indicators bolster the claim that excessive dependence on one technological actor, strategically or not, undercuts a state to autonomously defend and control its digital infrastructure and thus a core aspect of modern sovereignty.

Pakistan's Cybersecurity Landscape and Threat Assessment

At a time that is being shaped by the rapid development of artificial intelligence and competition among global powers in the cyber domain, Pakistan is experiencing the push and pull of both notable internal weaknesses and prevailing external geopolitical agendas in cybersecurity. The continuing tech tussle between the U.S. and China, especially in the area of AI, cyber capabilities, and surveillance technologies, is heightening Pakistan's geopolitical importance but also subjecting it to more rapid cybersecurity risks and dependencies (Khan, 2022).The pathway of digital regulation in Pakistan first started in the earlier years, such as the Electronic Transactions Ordinance passed in 2002, and later moved towards a more detailed regulation framework via the Prevention of Electronic Crimes Act (PECA) in 2016. PECA, which provided the legal infrastructure for prosecuting a range of cyber-related offences from data theft to cyberterrorism, has been criticised for its selective enforcement, lack of technology and misuse against political opponents.

Towards a more centralised and strategic approach, the National Cyber Security Policy (NCSP) released in 2021, suggested setting up a National Cybersecurity Authority and expanding the Computer Emergency Response Teams (CERTs). These are steps that stem from the recognition that digital threats are increasing, but implementation of these steps has been gradual, and coordination within institutions has been lacking. Pakistani cybersecurity threat landscape is directly framed by the technological policies of external actors, primarily China and the U.S, in a sense that the competition over AI and data dominance, indirectly affects NSE of Pakistan and has effects on Pakistan's digital infrastructure and its strategic choice. China has become an important partner for Pakistan in the technology markets, including AI-based surveillance systems, smart city projects, and telecommunications infrastructure under the China Pakistan Economic Corridor (CPEC), but such dependence is dangerous when it comes to matters of digital sovereignty, data security, and vulnerabilities of cyber-espionage. Without effective data protection legislation and in the absence of mature technology controls, these issues are exacerbated. While the Personal Data Protection Bill 2021 aims to plug some of these gaps, it is still in limbo and unenforced. Pakistan's institutional unpreparedness and systemic deficiencies have been highlighted by several high-profile cyber incidents. Various incidents such as the Habib Bank ATM scam of 2017, the cyberattack on the Federal Board of Revenue (FBR) of 2021, and the breach in 2023 at the National University of Sciences and Technology (NUST) showcase the absence of sufficient data security frameworks in both public and private sector organizations, respectively. These incidents have been happening in the context of growing regional tensions and global cyber competition in such a way that both state & non-state actors are now threatening Pakistan's digital infrastructure. Sensitive government and citizen data allegedly leaked on the dark web, and regional cyber espionage activities have also bolstered Pakistan's already complex security environment (Azhar, 2024).

The complexity of some geopolitical considerations in Pakistan's digital ecosystem is relevant to the U.S.-China AI race. With both the global super-powers locked in a race to create pre-existing AI ethics, governance, and cyber norms, Pakistan stands at the risk of existing solely as a consumer of imported technologies, without any institutional capacity to appraise, regulate or protect from them. Although Chinese AI systems are filling digital infrastructure gaps, the resulting strategic dependencies are unlikely to be sustainable in the long run. Simultaneously, low participation in U.S.-supported cybersecurity activities prevents Pakistan from gaining broader access to a variety of technical and regulatory frameworks. In this sense, when Pakistan does not play its due role in global discussions on artificial intelligence and cyberspace, it is merely over-responding to shifting external winds rather than shaping them. The cybersecurity reality in Pakistan is that there is a large gap between the high-flying policies drafted and the gloomy ground reality. Legal instruments and national strategies have been established, but their implementation is weak. Pakistan is thus vulnerable both to criminal threat, as it faces the brunt of international cyber-crime groups, but also more perniciously, to being made a battleground in a global war of rival powers, in an age of cyber warfare and AI driven espionage.

Digital Non-Aligned: Global South Examples

At a time when Pakistan must find its footing in the burgeoning strategic-technological competition between the United States and China, lessons from the Global South, specifically through the Vietnamese and Malaysian pathways, can shed light on how digital non-alignment may be pursued through a defensive realist lens. The vulnerability to repeated hacking has certainly tailored the approach Vietnam has taken in regard to cybersecurity to the one we have seen in action with groups like APT41 and Mustang Panda targeting critical state infrastructure such as airports and government ministries since 2015. In turn, Vietnam implemented a defensive strategy that fused institutional resilience with asymmetric countermeasures (Dong, 2025).It also restricted Huawei from 5G equipment, drove indigenous alternatives through Viettel's local chip production, and adopted the 2018 Cybersecurity Law to increase data sovereignty so that it was able to more closely control its data, conducted by companies. Establishing the military cyber unit called Force 47 and the

ambition to train 10,000cybersecurity professionals each year by 2030 highlights the understanding of how technological sovereignty rests not only on choosing the right hardware but also on building long-term capacity for defence against coercion in Vietnam. By contrast, Malaysia has chosen a more nuanced strategic hedging approach. It provides a framework under which some Chinese technologies, specifically from Huawei, can be incorporated, but only under stringent conditions, including NATO-grade encryption standards, while preserving security partnerships with the United States. A calibrated balancing act that allows Malaysia to gain economically from Chinese investment while retaining room for manoeuvre when the need for geopolitical de-escalation arises. As such, they provide a functional model for Pakistan. Just like Vietnam, Pakistan needs to improve institutional capacity and build domestic technology infrastructure to minimise its exposure to foreign interference. At the same time, as I argue in the case of Malaysia, engagement with both powers can be made conditional and reversible d thus retaining strategic flexibility. Over five years, for instance, phased diversification such as the replacement of 30 percent of Chinese digital systems with hybrid alternatives localised data laws, and selective partnerships with neutral actors (such as South Korea or the European Union) can help Pakistan conserve its autonomy rather than creating an impenetrable bubble that eliminates its remaining prospects for innovation. Following the defensive lessons of Vietnam and the strategic lessons of Malaysia, Pakistan can embrace a realistically non-aligned and resilient digital future (Hezril Azmin,2024)

Policy Recommendations and theWay Forward for Pakistan:

As the world pivots increasingly towards a technology ecosystem bifurcated by US-China competition, Pakistan needs to prepare for the technological future with a strategy that balances the need to protect national interests with the desire for national prosperity. Balancing its relations since it has strong relations with China (CPEC) and the US for defence and trade. Pakistan must base its strategic autonomy in this evolving landscape on long-term resilience, institutional reform and diversified partnerships. Pakistan needs to strengthen its institutional framework to insulate its digital ecology from external interference in the immediate term -a priority, no doubt, plausibly, in the foreseeable future. One of the key recommendations is to establish a National AI Security Task Force to "identify, regulate, and help integrate foreign technology" into "national critical infrastructure." Such a body could oversee technology imports, weigh national security compliance, and act as a bulwark against threats from geopolitical rivalries, most notably the U.S.-China AI competition. Next up is the passing of an all-encompassing data sovereignty law. If all data about Pakistani citizens is stored and processed only inside the country, then Pakistan will become less vulnerable to external surveillance and political pressure. The new legal regime must be in line with international practice, but ground realities in Pakistan regarding the security of Pakistan and socio-political situation shall also be kept in view. At the same time, it is necessary to invest in local encryption standards. Through the responsible engagement of technical universities within Pakistan, cybersecurity firms, and government-funded research institutions, not only will encryption tools, like the end-to-end encryption we see today, but also tools that are designed and applied locally and to international security standards be developed while being free from the dependency of foreign platforms. This, in turn, strengthens data protection, privacy and domestic control over sensitive communications (Javed, 2021).

Pakistan has to expand its local capacity and investment in local innovation to reduce its dependence on any global power in terms of technology. One important development would be the creation of a Cyber Defence Fund to give a few per cent of GDP for R&D in cybersecurity. The prosperity this capital outlay would promote would also encourage innovation, global talent flow to Canada, and long-term security dividends. Educational reforms to build skills in important areas are needed to help sustain this work. Engineering and computer science programs need to be updated to integrate AI, cybersecurity, and quantum computing. Public universities can be targeted to meet the AI specialist production figures every year, with scholarships, research grants, and exchange programs funded by the government. At the same time, Pakistan has to

broaden the spectrum of those technological partnerships. Even though relations with China are primarily strategic, dependency on a single player has geopolitical risk. Thus, increased cooperation with neutral, technologically advanced states like South Korea, the UAE, and Germany would provide access to different innovations while fostering less political entanglement. This kind of multi-vector engagement can improve resilience and send a clear message of Pakistan's dedication to neutrality in digital matters. Pakistani strategy in the long run should be according to the pattern of building an independent AI. Adopt a National AI Initiative to develop and promote home-based AI research, start-ups, and innovation hubs. Such government incentives can facilitate public-private collaboration, accelerate the commercialisation of AI products, and reduce reliance on foreign solutions. Not only would sovereign capability provide digital sovereignty, but it would also facilitate having a competitive advantage for Pakistan in regional and global markets (Ali, 2020). Pakistan also needs to play its part in the AI and cybersecurity global governance forums. Setting international standards for the digital economy should also be an area where Pakistan actively participates to ensure that digital norms reflect its interests. Multilateral engagement in global organisations like the UN, GGE and the GPAI would also increase Pakistan's voice in the global debate on ethical use of AI, governance of cybersecurity, and data privacy.

Pakistan must take the lead in creating a South Asian Cybersecurity Pact at the regional level. A multilateral agreement of this kind would enable South Asian countries to exchange threat intelligence, harmonise regulatory regimes, and carry out cooperative incident responses to regional cyber events. This may act as confidence-building measure and enable Pakistan to take a lead role in advancing regional digital resilience on the subcontinent (Khan, 2022). However, in addition to bolstering domestic institutions, Pakistan needs to refocus its foreign policy to cope with the great-power competition. Its deep economic and infrastructural ties with China through CPEC are still the mainstay, but over-reliance may create vulnerabilities. Pakistan, for its part, relies on its defence cooperation with the U.S. and access to U.S. export markets as core components of its strategic calculus. To protect its status, Pakistan ought to leverage its connections to the U.S. and evolve its bilateral engagement beyond just security assistance and aid. Improved access to American markets via instruments like the Generalised System of Preferences (GSP) could encourage exporters to diversify out of commodities and decrease economic dependence on Chinese-financed projects. Such an economic rebalancing would also defuse external pressure on Pakistan to reform at home. Simultaneously, Pakistan must conduct transparent diplomacy with China. Pakistan can prevent Western democracies from leaning towards a contentious stand on issues such as Hong Kong or the treatment of Uyghur Muslims by not overaligning itself with China on such issues. Appointing civilian head of the CPEC Authority and being more transparent about CPEC agreements will ease concerns in the region and allow for more public buy-in

Digital Non-Alignment and Strategic Autonomy:

Pakistan’s future trajectory should be guided by the principle of digital non-alignment meaning that Pakistan needs to pursue its own national goals even while remaining neutral during the tech cold war. A strategic balance of worsening relations between the two superpowers, Pakistan can benefit from both without becoming a battleground proxy to either one. In pursuing those objectives, Pakistan clearly needs to take immediate measures to protect its digital sovereignty, resilience and reliance by forming new alliances and investing in innovation for the long-term. A well-defined framework that combines proactive diplomacy, technology investment, and regional collaboration would position Pakistan as a sovereign digital power, capable of preserving its national interests while also contributing substantially to global digital governance.

Conclusion

The AI arms race between the US and China is defined as the contest of the 21st century, and, indeed, it does transcend the conventional boundaries of geopolitics and underpins pillars of economic security, military

capacity and national sovereignty. This competitive backdrop has bred a contradictory situation for Pakistan: on the one hand, partnerships with China have fast-tracked its digital transformation through projects like CPEC, but on the other hand, they have fostered dependencies that hamper agency in the long run. On the other end, alignment with U.S. technology ecosystems while providing a form of comprehensive security architecture comes with geopolitical strings and sanctions risks. This dilemma is explained by defensive realism, as Pakistan's cybersecurity deficiencies are symptoms of a more proverbial structural anarchy, where, as defensive realists argue, the need of secondary states is to survive by being pragmatic in strategy-making that focuses on capabilities instead of ideologies (i.e., balancing, band wagoning, etc.). The significance of this finding is even more pronounced concerning Pakistan. The dependence on Chinese infrastructure producers (92% of telecom networks), shallow institutional defences (number 67 in global cybersecurity indices), means that it is vulnerable to two types of threats, namely external coercion by great powers, and cyber operations by regional adversaries like India. Attention-grabbing breaches-from the FBR tax database breach to cyber espionage campaigns waged by nation-states-highlight the systematic deficiencies in data governance and technical capability. Alarming national strategies, disjointed application systems, and an acute dearth of expertise can make this problem worse.

But Pakistan does have some agency here. The policy framework outlined here, with its grounding in the strategic moderation implied by the tenets of defensive realism, is a realistic avenue towards digital non-alignment. Short-term solutions such as quantum-safe encryption and data sovereignty legislation can alleviate existential threats in the near term; medium-term investments in education and R&D (Cyber Defence Fund, etc.) are a commitment to building indigenous resilience. Participating in global AI governance as well as regional cyber pacts on a long-term basis, it is said, can motivate Pakistanis to become a norm-shaper instead of merely a foreign technology consumer. Most importantly, diversification of partners beyond either superpower involving neutral states like South Korea and the UAE, would lessen overreliance on one superpower. Yet, the stakes are also greater than Pakistan. For developing states, this holds even more significance as their decisions today will shape their position in the future digital order, with AI as the new currency of power. For Pakistan, the way forward neither entails submission to Chinese technological dominance nor wholesale acceptance of Western paradigms; instead, a sovereign approach based on self-reliance, institutional strength, and defensive posture is warranted. Pakistan can attempt to manage the U.S.-China rivalry not as a battleground but as an actor acting on its own if it embraces this approach, ensuring the digital future while maintaining the country's geopolitical independence. And, in a time when data is the new oil and algorithms the new arms, to have an option of technological sovereignty is the conditio sine qua non to live in the time of AI.

References

Ali, S. M. (2020, December 1). *The U.S.-China Strategic Rivalry and Its Implications for Pakistan • Stimson Center*. Stimson Center. https://www.stimson.org/2020/the-u-s-china-strategic-rivalry-and-its-implications-for-pakistan/

Azhar, A., (2024, July 18). *Pakistan's Limited Role in AI and Its Implications for National Security — Global Defense Insight*. Global Defense Insight. https://defensetalks.com/pakistans-limited-role-in-ai-and-its-implications-for-national-security/

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Dong, J. (2025). *AI: China and the US go head-to-head | Lowy Institute*. Lowyinstitute.org. https://www.lowyinstitute.org/the-interpreter/ai-china-us-go-head-head

Govt. of Pakistan. (2021). *Government of Pakistan National Cyber Security Policy 2021*. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

Javed, Z. (2021). The role of artificial intelligence in the enhancement of cyber security of Pakistan. *Journal of Contemporary Studies*, *10*(2), 1-14.

Khan, M. N. (2022). Pakistan and Russia's Convergence of Interests in the Emerging Geopolitical Environment. *Journal of Security & Strategic Analyses*, *8*(2), 27-52. https://doi.org/10.57169/jssa.008.02.0191

Obaid, M. (2023). *PTA Issues Cyber Security Strategy 2023-2028 for Pakistan's Telecom Sector: A Five Year Plan Towards Digital Resilience*. Pta.gov.pk. https://pta.gov.pk/index.php/category/pta-issues-cyber-security-strategy-2023-2028-for-pakistans-telecom-sector-a-five-year-plan-towards-digital-resilience-980103515-2024-07-04

Sacks, S. (2022, June 3). *China's Emerging Cyber Governance System | China Cyber Outlook | CSIS*. Www.csis.org. https://www.csis.org/programs/strategic-technologies-program/resources/china-cyber-outlook/chinas-emerging-cyber

Sarfraz, H. (2025, February 9). *AI becomes the latest flashpoint in the US China rivalry*. Tribune.com.pk; The Express Tribune. https://tribune.com.pk/story/2527387/ai-becomes-the-latest-

Yildirim, A. G. (2025). *US-China AI race in full throttle as both sides strive for dominance*. Aa.com.tr. https://www.aa.com.tr/en/americas/us-china-ai-race-in-full-throttle-as-both-sides-strive-for-dominance/3545553