ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 03 No. 02. Apr-Jun 2025.Page#.2123-2134
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

Armed with Algorithms: U.S.-China Tech Rivalry and Its Strategic Implications for Pakistan

Amna Ambreen Khalid
Mphil Scholar IR, University of Management and Technology, Lahore
amnak.1703@gmail.com

Abstract
As the global order transitions from industrial-era geopolitics to algorithm-driven security architectures, the United States and China are emerging as the principal actors in a high-stakes race for technological supremacy. This article examines the strategic rivalry between these two powers through the lens of algorithmic warfare and advanced technological competition. It further investigates how this competition reshapes the security environment for peripheral states, particularly Pakistan. The article, using International Relations theory as well as cyber-security and strategy literature, discusses Pakistan's unique situation within the context of ever-evolving digital dependencies, cyber vulnerabilities, and geo-strategic partnerships. Islamabad's policy landscape is swiftly changing with America's increasing stranglehold over global semiconductor and AI technology along with China's massive investment through CPEC's Digital Corridor. The article also analyzes the impact on Pakistan's military doctrine and cyber sovereignty alongside other critical national security concerns.

Keywords: U.S.-China tech rivalry; digital geopolitics; artificial intelligence; cyber governance; Pakistan; emerging technologies; digital sovereignty; cybersecurity; strategic competition; Belt and Road Initiative.

INTRODUCTION:

In today's world, power isn't just about who has the biggest nuclear arsenal or the strongest army anymore. Instead, it's increasingly about who leads the race in cutting-edge technologies like artificial intelligence, big data, cyber warfare, and quantum computing. We're entering an era where machines and algorithms don't just support decisions—they can drive entire military operations. This shift is changing how countries think about security and influence.

At the heart of this new technological rivalry are the United States and China. These two giants aren't just competing over trade or traditional military strength—they're battling for dominance in everything from 5G networks and semiconductor production to AI-powered weapons and digital surveillance. But this isn't just a contest between two countries; the ripple effects reach all around the world, reshaping alliances and forcing many nations, especially in the Global South, to rethink their strategies and partnerships.

Take Pakistan, for example. Located at the crossroads of South Asia, Central Asia, and the Middle East, Pakistan finds itself caught in the middle of this high-tech contest. On one hand, it has a long-standing defense relationship with the U.S.; on the other, it's deepening economic ties with China, especially through big projects like the China-Pakistan Economic Corridor (CPEC). While

China's investments bring new digital infrastructure and advanced surveillance tech, Pakistan also faces risks—from cyber attacks to becoming overly dependent on foreign technologies. Navigating these challenges requires a delicate balancing act.

This article takes a closer look at the fierce tech competition between the U.S. and China through the lens of "algorithmic warfare" and explores what it means for Pakistan. By understanding how global tech trends intersect with geopolitics and Pakistan's own capabilities, we hope to uncover both the opportunities and the dangers that lie ahead in this new digital battleground.

Literature Review

The rising technological rivalry between the U.S. and China signals a major shift in how global power is contested today. Technologies like artificial intelligence, 5G, and semiconductors have moved beyond just tools of innovation—they've become critical levers of national security and influence. As Adam Segal points out, this competition is "less about trade and more about ideology and influence," highlighting that it's not just economic interests at play but competing visions for the future world order (Segal, 2018, Council on Foreign Relations).

In the same vein, political analyst Mathieu Rolland explains that these emerging technologies are deeply embedded in broader national strategies and ideological narratives, shaping how countries project power and dominance on the global stage. One clear example is China's Digital Silk Road (DSR), which builds upon the Belt and Road Initiative by exporting digital infrastructure and governance models to other countries. According to Zeng Lingliang, the DSR is not just an economic project but also a political tool extending China's influence, especially in developing countries seeking digital connectivity (Zeng, 2021, Carnegie Endowment).

Jonathan Hillman warns that China's export of surveillance systems and AI technology could accelerate the spread of "digital authoritarianism" —a form of governance where technology is used to monitor and tightly control populations This demonstrates how technology influences not just economies and infrastructure but also political freedoms and social norms. This raises questions about sovereignty, digital dependency, and human rights, especially in fragile democracies.

Pakistan, as a primary partner in the China-Pakistan Economic Corridor (CPEC), is heavily reliant on Chinese digital infrastructure, including fiber optic cables and smart surveillance systems. Ahmed (2022) warns that this deepening digital reliance may translate into long-term strategic vulnerability (Ahmed, 2022). Similarly, Khan critiques the lack of public debate over data ownership, surveillance, and regulatory control, which threatens Pakistan's digital sovereignty (Khan, 2021).

Pakistan's Digital Pakistan vision and National Cybersecurity Policy are early steps toward asserting digital sovereignty. However, think tanks such as Carnegie Endowment and Atlantic Council suggest that these efforts are undermined by weak institutional coordination and inadequate cyber infrastructure. The Carnegie Endowment report (2023) emphasizes the need for stronger public-private partnerships and data protection laws (Carnegie, 2023). Meanwhile, Atlantic Council highlights Pakistan's dependence on foreign tech firms and donor-driven policies as limiting factors (Atlantic Council, 2022).

Literature increasingly points to the possibility of non-aligned digital diplomacy by middle powers like Pakistan. Pauwels (2023) argues that digital non-alignment can be pursued through diversified partnerships, policy interoperability, and participation in multilateral forums (Pauwels, 2023). Nonetheless, scholars caution that domestic structural issues—such as elite

capture, low R&D investment, and bureaucratic inefficiency—limit Pakistan's ability to chart an autonomous digital course.

Theoretical Framework

Understanding the implications of the U.S.-China tech rivalry on Pakistan requires grounding in International Relations (IR) theory—particularly those frameworks that accommodate asymmetries of power, emerging technologies, and global interdependence. This article draws on three complementary theoretical approaches: **Neorealism**, **Dependency Theory**, and **Technological Constructivism**. Each contributes to a deeper understanding of Pakistan's strategic dilemmas and limited autonomy in an algorithmically restructured world.

1. Neorealism (Structural Realism)

Neorealism posits that the international system is anarchic, and states act rationally to ensure their survival by maximizing power relative to others (Waltz, 1979). In the context of technological competition, power is no longer measured merely in terms of military hardware or GDP, but also in terms of control over advanced technologies, data infrastructure, and cyber capabilities.

From a neorealist lens, both the U.S. and China are engaging in power-maximizing behaviors to ensure dominance in emerging domains like AI, space, and quantum computing (Kaplan, 2021). This rivalry resembles a classic security dilemma: one state's digital advancement provokes countermeasures from the other, leading to an arms race in cyberspace and algorithmic warfare. For peripheral states like Pakistan, this rivalry reduces strategic options and increases vulnerability, as aligning with one great power may invite suspicion or reprisal from the other.

2. Dependency Theory

Originating from Latin American scholarship, Dependency Theory argues that peripheral states are structurally constrained by their reliance on the core for technological, economic, and institutional support (Frank, 1966). This dependence perpetuates underdevelopment and limits sovereignty.

Pakistan, heavily reliant on Chinese technological infrastructure (e.g., Huawei's involvement in CPEC) and international financial institutions dominated by the West, exemplifies a dual dependency model. Its adoption of Chinese digital surveillance tools raises concerns about digital colonialism and reduced data sovereignty (Feldstein, 2019). Meanwhile, efforts to maintain economic relations with Western markets restrict Pakistan's ability to fully pivot toward China.

This dynamic suggests that rather than benefiting equally from globalization or multipolarity, Pakistan is caught in a web of technological dependencies that constrain its strategic autonomy.

3. Technological Constructivism

While neorealism and dependency theory emphasize structural constraints, constructivist approaches underscore the social dimensions of technology—how ideas, norms, and identities shape the adoption and application of technology (Adler, 2005). In this view, technology is not neutral; it carries embedded ideologies and institutional logics that influence state behavior.China's digital engagement with Pakistan—ranging from AI-based surveillance systems to the Digital Silk Road—comes with an implicit model of cyber-governance: centralized, opaque, and security-heavy (Creemers, 2021).

The competition over technology in Pakistan isn't just about which gadgets or systems the country adopts—it's also about the deeper values and governance models that these technologies bring with them. Will Pakistan's digital future mirror China's tightly controlled,

centralized system? Or will it carve out a hybrid path that balances innovation with democratic checks and safeguards?

To better understand Pakistan's position in the U.S.-China tech rivalry, this article draws on three important theoretical perspectives. Neorealism sheds light on the security concerns driving state behavior, emphasizing the struggle for power and survival in an anarchic international system (Waltz, 1979). Dependency theory highlights how economic and technological dependencies shape the strategic choices of developing countries like Pakistan (Frank, 1967). Lastly, technological constructivism explores how technology is not neutral but embedded with social norms and political values, influencing how states and societies interact.

Together, these lenses help frame the complex realities of algorithmic warfare and its potential consequences for Pakistan's sovereignty and governance.

Understanding Algorithmic Warfare

In the 21st century, warfare is changing dramatically, moving beyond traditional battlefields into digital arenas controlled by algorithms. Algorithmic warfare describes how artificial intelligence, big data, autonomous systems, and cyber tools are increasingly woven into military strategies, decision-making, and operations. This shift isn't just about new technology—it's reshaping how wars are fought, speeding up conflicts, expanding their reach, and raising fresh ethical questions.

1. Defining Algorithmic Warfare

Algorithmic warfare involves leveraging machine learning and data-driven algorithms to process intelligence, monitor targets, guide unmanned systems, and make real-time battlefield decisions. A significant initiative in this domain is the U.S. Department of Defense's Project Maven, established in 2017. This project integrates artificial intelligence to analyze drone footage, enhancing target identification capabilities. Initially, Google provided TensorFlow software to assist in this effort, though the company later withdrew due to internal employee concerns. Subsequently, Amazon and Microsoft secured contracts to continue similar work, focusing on object recognition and data analysis for aerial surveillance (Brewster, 2021, Forbes; Byford, 2018, The Verge).

In parallel, China has incorporated AI into its military strategy through the concept of "military-civil fusion." This approach integrates civilian technological advancements into military applications, encompassing areas such as surveillance systems, autonomous drone swarms, and predictive policing tools. These developments are part of China's broader initiative to modernize its military capabilities and enhance its technological infrastructure.

This technological transformation promises increased speed, precision, and situational awareness in military operations. However, it also introduces complex ethical and strategic challenges, including questions about decision-making accountability, the potential for autonomous escalation, and the implications of AI-driven warfare on international norms and human rights.

2. Key Components of Algorithmic Warfare

AI enables predictive analysis and autonomous decision-making based on vast datasets. In military use, this translates to predictive targeting, anomaly detection, and dynamic threat assessment. China's AI research has increasingly focused on military applications, with institutions like the PLA's Strategic Support Force advancing deep learning models for electronic warfare and space surveillance (You, 2022).

From the U.S. MQ-9 Reaper drones to China's GJ-11 stealth drones, unmanned aerial vehicles (UAVs) are a central feature of algorithmic warfare. These systems are now being equipped with AI, allowing for swarm tactics, autonomous flight, and precision strikes—without requiring continuous human control.

Algorithmic warfare also encompasses the cyber domain. Cyberattacks are no longer merely about data theft; they now target military infrastructure, satellite networks, and AI systems themselves. The Stuxnet worm, allegedly developed by U.S. and Israeli agencies to sabotage Iranian nuclear facilities, demonstrated the power of software as a strategic weapon (Zetter, 2014). China, too, has developed robust cyber units capable of both offense and defense, with Pakistan caught in the geopolitical crossfire of competing digital doctrines.

3. Strategic Advantages and Risks

The integration of algorithms into warfare offers tactical benefits: speed, automation, and reduced human risk. However, it also creates strategic vulnerabilities:

- **Escalation Risks:** Automated systems can misinterpret signals, leading to unintended conflict escalation.
- **Opacity and Accountability:** AI-driven decisions can be opaque even to their operators, raising concerns about legal responsibility and proportionality under international law.
- **Techno-nationalism:** The race to dominate algorithmic warfare fuels techno-nationalism, where control over proprietary algorithms becomes a marker of sovereignty and power.

4. The U.S.-China Race in Algorithmic Warfare

Both the U.S. and China see AI as central to future warfare. The U.S. National Security Commission on Artificial Intelligence warned in 2021 that losing the AI arms race would jeopardize national security (Schmidt & Work, 2021). China's 2017 AI development plan explicitly aims to become the world leader in AI by 2030.

This competitive landscape pushes both nations to rapidly militarize emerging technologies, often without sufficient ethical oversight or global regulation—leaving smaller states like Pakistan in a precarious position.

U.S.-China Tech Rivalry: Origins and Trajectories

The U.S.-China technological rivalry has evolved into one of the defining features of contemporary geopolitics, characterized by escalating competition for supremacy in strategic technologies such as artificial intelligence (AI), 5G telecommunications, semiconductors, quantum computing, and cyber capabilities. The origins of this rivalry trace back to China's rapid economic ascent in the early 2000s, marked by strategic state-led initiatives like the "863 Program" and the more ambitious "Made in China 2025" plan. China's efforts to reduce its reliance on foreign technology and become a high-tech leader have fueled the rise of major firms like Huawei, ZTE, Alibaba, and Tencent. As these companies expanded globally, the U.S. began to see China's technological ascent not just as economic rivalry, but as a direct challenge to its dominance and national security.

This concern led to major policy changes in Washington—such as export controls on semiconductors, bans on Chinese tech firms in U.S. markets, and pressure on allies to keep Chinese vendors out of key infrastructure projects, especially in 5G networks. Actions like the Huawei ban and restrictions on China's access to cutting-edge semiconductor technology from firms like TSMC, ASML, and Nvidia marked a clear shift toward techno-nationalism. In response,

China doubled down on domestic innovation, investing heavily in chip development, AI, and military tech to boost self-reliance.

This competition now transcends national borders, reshaping global supply chains, standards, and technological alliances. Countries are increasingly being pushed to pick sides between the American and Chinese digital ecosystems—particularly in areas like digital infrastructure, surveillance tools, and cloud platforms. For developing nations such as Pakistan, the stakes are high. Pakistan depends significantly on Chinese technology through initiatives like the China-Pakistan Economic Corridor (CPEC), yet it also values its longstanding relationship with the United States for defense cooperation and development aid.

More fundamentally, this tech rivalry reflects a deeper ideological divide. It pits a U.S.-led vision rooted in open markets and transparency against China's model of state control, data sovereignty, and centralized digital governance. The conflict is as much about values and norms as it is about technology and economics. For policymakers in countries like Pakistan, understanding the roots and direction of this rivalry is essential. Navigating this terrain requires a delicate balance of seizing economic opportunities, safeguarding national security, and aligning diplomatically in a world increasingly split along technological lines.

Pakistan's Technological Positioning in a Polarized World

As the tech rivalry between the U.S. and China intensifies, Pakistan finds itself in a complex position. While it hasn't yet emerged as a leader in advanced areas like artificial intelligence or algorithmic warfare, its strategic location and international ties make it significantly influential. It plays a crucial role in China's Belt and Road Initiative (BRI) while also maintaining deep-rooted connections with the U.S.-led security framework. This dual alignment presents both opportunities and challenges as Pakistan navigates an increasingly dynamic global tech environment.

1. Technological Dependence and Asymmetry

Pakistan's national security and digital infrastructure are heavily reliant on foreign technologies. The country imports most of its surveillance systems, communications hardware, and defense-related software from either China or Western suppliers. This asymmetrical dependence places Pakistan in a reactive rather than proactive position in the global tech race. While China provides critical digital infrastructure through projects like the China-Pakistan Economic Corridor (CPEC), it also introduces dependency on Chinese systems and cyber protocols (Small, 2020).

For instance, Pakistan has adopted Chinese-origin smart surveillance tools, including facial recognition technologies and city-wide monitoring systems. These are marketed under China's "Safe City" model, which itself is a product of algorithmic and AI-powered infrastructure (Hillman &McCalpin, 2019). While such tools promise improved internal security, they also raise concerns about digital sovereignty and data governance.

2. Civil-Military Synergy in Technological Development

Pakistan's defense establishment has historically led innovation, particularly in missile technology, nuclear deterrence, and strategic communications. However, in algorithmic warfare, the gap between civilian and military technological development is widening. Unlike China's model of "military-civil fusion," Pakistan lacks structured institutional pathways to integrate civilian tech innovation with military modernization (Ahmad, 2022).

Despite growing domestic interest in AI, institutions like the National Center of Artificial Intelligence (NCAI) and various public-sector universities remain underfunded and under-

coordinated. Pakistan's AI Policy 2022 while a step in the right direction falls short of linking algorithmic technologies with national security planning.

3. Digital Geopolitics: Between Silicon Valley and Shenzhen

As U.S.-China competition intensifies, Pakistan finds itself caught between two competing digital ecosystems:

- **The U.S. Model** emphasizes open-source innovation, regulatory governance, and democratic accountability. However, Pakistan's political mistrust of Western oversight (especially in cybersecurity and data localization) limits deeper integration into this model.
- **The Chinese Model** offers turnkey technological solutions with minimal governance requirements. China's digital exports to Pakistan are bundled with strategic partnerships—often under the guise of "technological sovereignty"—but at the cost of data autonomy and potential surveillance risks (Chin, 2020).

This dichotomy places Pakistan in a challenging position: pursue Western tech partnerships and risk strategic frictions with China, or deepen digital ties with China and compromise on transparency and standards (Segal, 2018).

4. Cybersecurity Vulnerabilities and Strategic Exposure

Pakistan's increasing reliance on algorithmic and networked systems makes it vulnerable to cyber threats, espionage, and technological sabotage. Recent attacks on Pakistan's financial and telecom sectors underscore the growing threat landscape. Yet, there is no comprehensive cybersecurity doctrine or inter-agency coordination framework to secure the country's digital infrastructure (Shahid, 2021).

Moreover, Pakistan lacks indigenous capabilities in cyber offense and defense, which are critical components of algorithmic warfare. In the absence of this capacity, Pakistan becomes reliant on bilateral partnerships for digital security—further constraining its autonomy.

Case Studies: Navigating Strategic Choices Between U.S. and China

Case Study 1: Huawei and Pakistan's 5G Dilemma

In 2020, Pakistan began exploring 5G deployment, with Chinese tech giant Huawei positioned as the primary contender. While cost-effective, Huawei's involvement drew warnings from the United States over national security and espionage concerns (Brookings Institution). Several Western allies banned or restricted Huawei; Pakistan, however, hesitated and chose a cautious approach—neither endorsing Huawei publicly nor banning it outright.

This cautious neutrality reflects Pakistan's strategy to avoid alienating either the U.S. or China while delaying irreversible tech commitments (Carnegie Endowment for International Peace).

Case Study 2: Safe City Projects and Surveillance Partnerships

Pakistan's Safe City projects, particularly in Lahore and Islamabad, have been driven by Chinese firms like Huawei and Hikvision. These systems include AI-powered facial recognition and license plate detection technologies. Civil rights watchdogs have raised concerns about mass surveillance and lack of data protection laws (Amnesty International).

Meanwhile, U.S. officials have expressed unease about the use of Chinese surveillance technologies in allied countries, citing data security and geopolitical risks (Council on Foreign Relations).

Case Study 3: AI in Military Applications and Civil-Military Fusion

China's national strategy emphasizes civil-military fusion (CMF), encouraging synergy between civilian AI firms and the military. Pakistan has yet to replicate this model in a formalized way, although the Pakistan Army has initiated AI labs and drone units.

- The **National Centre for Artificial Intelligence (NCAI)** operates primarily in academia without structured links to defense planning (NCAI official site).
- China's defense collaborations with Pakistan include joint research and tech-sharing initiatives that imply a soft transfer of civil-military integration practices (Jamestown Foundation).

Case Study 4: Technology Transfer under CPEC vs. U.S. Knowledge Aid

China's digital projects under the China-Pakistan Economic Corridor (CPEC) have created infrastructure such as fiber optics, e-governance systems, and digital TV (CFR: Digital Silk Road). However, these projects often lack meaningful technology transfer, leaving Pakistan dependent on Chinese expertise.

In contrast, the U.S. approach centers on capacity-building—through scholarships, educational exchanges, and R&D grants—offering longer-term benefits to human capital development (USAID Pakistan).

Strategic Implications for Pakistan

As Pakistan navigates the deepening technological divide driven by U.S.-China rivalry, its strategic independence, digital sovereignty, and long-term development path hang in the balance. The choices made today will shape the nation's technological capabilities, cybersecurity strategies, global partnerships, and innovation landscape for generations to come.

1. Technology Dependence and Digital Sovereignty

Pakistan's growing reliance on Chinese infrastructureranging from telecommunications to surveillanceposes serious questions about its digital sovereignty. Chinese companies not only provide hardware but also often maintain control over software updates, system architecture, and even data routing (Chaudhry, 2022).

While U.S. technologies offer alternatives, they often come with compliance constraints (e.g., export control laws, vetting requirements), making integration into U.S.-led tech networks more difficult for countries with complex political ties, such as Pakistan (Export.gov).

Implication: Pakistan must strike a balance between digital capacity building and strategic independence, possibly by developing indigenous alternatives or enforcing data localization and sovereignty-enhancing policies.

2. Cybersecurity Risks and the Intelligence Landscape

With digital expansion comes the growing threat of cyber espionage and digital sabotage. Pakistan's dependence on foreign technologies, especially from China, places it within contested cyber geographies. U.S. intelligence reports have regularly flagged the use of Chinese digital platforms in potential surveillance (ODNI Annual Threat Assessment, 2023).

At the same time, Pakistan lacks a comprehensive national cybersecurity strategy that can systematically monitor, audit, and defend its digital infrastructure from external and internal threats (Pakistan Ministry of IT & Telecom, 2022).

Implication: Pakistan's security apparatus must broaden its focus to include emerging digital threats beyond conventional warfare, ensuring cyber defense becomes a national security priority.

3. Strategic Autonomy and Diplomatic Tightrope

The U.S.-China tech rivalry forces states like Pakistan into strategic decisions with long-term consequences. While China offers accessible and less conditional infrastructure, the U.S. remains a critical source of investment, diaspora networks, and institutional support, particularly in higher education and governance reform.

Pakistan's attempt to balance both powers—exemplified in its silence on U.S. sanctions against Huawei and participation in both Chinese and Western digital platforms—exposes it to strategic vulnerabilities. Leaning too heavily on one side may jeopardize alliances or development aid from the other (Small, 2020).

Implication: Pakistan's foreign policy must institutionalize "tech diplomacy," creating agile frameworks for engaging with both powers without becoming a pawn in their rivalry.

4. Economic Modernization vs. Strategic Risk

CPEC's Digital Corridor offers Pakistan the promise of economic modernization, improved logistics, and integrated trade systems. However, this model lacks the transparency and multilateral checks and balances present in Western partnerships (CSIS, 2021).

Moreover, there are concerns that Pakistan's market is being used as a testing ground for Chinese technologies that do not meet global standards in cybersecurity or privacy. In contrast, the U.S. and allies promote regulatory frameworks aligned with democratic norms and human rights (Freedom House, 2022).

Implication: Pakistan needs a national regulatory and ethical framework for technology adoption that aligns with global standards to protect its consumers and institutions.

Here is the **Case Studies** section for your journal-style article *"Armed with Algorithms: U.S.-China Tech Rivalry and Its Strategic Implications for Pakistan."*

Case Studies: Navigating the U.S.-China Tech Rivalry

To better understand how countries like Pakistan can strategically position themselves in the evolving tech rivalry between the United States and China, it is valuable to study how other states—particularly middle and emerging powers—have navigated similar dilemmas. This section presents **three comparative case studies**: Vietnam, Turkey, and Indonesia.

1. Vietnam: Strategic Hedging and Digital Sovereignty

Background: Despite being a neighbor of China and maintaining strong economic ties, Vietnam has shown caution in adopting Chinese technologies, especially in critical infrastructure.

Key Strategies:

- Vietnam rejected Huawei from its 5G rollout, favoring local firms like Viettel and partnerships with Ericsson and Nokia (Reuters, 2020).
- The government has pursued a "Make in Vietnam" digital transformation policy to build domestic tech capacity.
- Maintains close security cooperation with the U.S., while also managing trade with China.

Implications for Pakistan:

- Pakistan can learn from Vietnam's balancing act, particularly in **limiting tech dependency** without severing strategic partnerships.
- Local innovation and **military-led tech development** (like Viettel) offer a model for Pakistan's defense and civilian sectors.

2. Turkey: Digital Autonomy and Regional Power Projection

Background: A NATO member with increasingly strained U.S. ties, Turkey has sought technological self-sufficiency while engaging with both Western and non-Western powers.

Key Strategies:

- Developed its own drone technology (Bayraktar TB2) with minimal reliance on Western parts (Brookings, 2022).
- Introduced strict data localization and cybersecurity laws, signaling a turn toward digital sovereignty.
- Balances Huawei's presence with European alternatives in telecom infrastructure.

Implications for Pakistan:

- Turkey's success in **dual-use technology** (civilian + military) and **tech diplomacy** illustrates a viable model.
- Emphasizing local defense tech and **independent foreign policy** in digital matters can guide Pakistan's approach.

3. Indonesia: Multipolar Engagement and Data Governance

Background: As Southeast Asia's largest economy, Indonesia has attempted to maintain neutrality amid U.S.-China tensions, focusing on domestic development and regional leadership.

Key Strategies:

- Engaged both Chinese (Huawei, Alibaba) and U.S. firms (Google, Microsoft) in building digital infrastructure.
- Introduced a **Personal Data Protection Law** in 2022, modeled partially on the EU's GDPR (Jakarta Post, 2022).
- Invested in national data centers and cloud sovereignty.

Implications for Pakistan:

- Indonesia demonstrates how strong legal frameworks and clear regulations can support multi-alignment while preserving national control.
- Pakistan can implement comparable legal reforms to safeguard its digital sovereignty while staying receptive to foreign investment.

Policy Recommendations for Pakistan

Amid the shifting landscape of the U.S.-China tech rivalry, Pakistan stands at a pivotal crossroads. With rising digital aspirations but limited homegrown technological capabilities, the country must pursue a carefully crafted and strategic policy path. The following recommendations are designed to help Pakistan seize emerging opportunities while mitigating potential strategic risks.

1. Adopt a Multi-Vector Tech Diplomacy Approach

Pakistan should refrain from aligning exclusively with any single technological bloc. Despite its strong strategic and economic relations with China, it's essential to keep communication open with the U.S. and other Western tech centers to maintain access to global innovations and markets. Adopting a multi-vector diplomatic approach will help minimize dependency and provide greater flexibility in policy-making.

2. Develop a National Tech Sovereignty Framework

This includes:

- Investing in local R&D institutions and universities.
- Encouraging public-private partnerships.
- Formulating data protection laws aligned with international norms.

3. Strengthen Cybersecurity and AI Governance Infrastructure

Pakistan must enhance national cybersecurity through:

- Establishing a central cyber command authority.
- Collaborating with international cybersecurity organizations.
- Training a cadre of experts to detect and counter AI-driven threats.
- Developing clear ethical guidelines for AI use in defense and civilian sectors.

4. Upgrade Technical and Vocational Training in Emerging Tech

To prepare for a technology-driven future, Pakistan needs to embed coding, AI, data science, and robotics into its technical education system. Closing the skills gap will empower young people and drive the growth of a knowledge-based, innovation-focused economy.

5. Leverage the China-Pakistan Economic Corridor (CPEC) for Tech Transfer

Pakistan should work to include targeted provisions in CPEC Phase II agreements that encourage technology transfer, support joint ventures, and facilitate the creation of Special Technology Zones (STZs) in key industries such as fintech, clean energy, and telecommunications.

6. Promote Strategic Autonomy in Digital Infrastructure

Dependence on foreign infrastructure presents long-term vulnerabilities. Pakistan needs to broaden its sources of digital infrastructure and prioritize investments in domestic cloud services, data centers, and telecommunications technologies.

7. Engage in Regional Tech Cooperation

Pakistan can enhance regional technological cooperation by engaging with platforms such as the Shanghai Cooperation Organisation (SCO) and the South Asian Association for Regional Cooperation (SAARC). Collaborative efforts in areas like data security, cyber norms, and AI ethics can strengthen shared resilience.

8. Institute a Technology Risk Assessment Framework

A dedicated national commission or task force should be established to continuously evaluate the potential risks and advantages of integrating specific foreign technologies, especially in critical areas such as defense, healthcare, and finance.

Conclusion

The rapidly escalating tech rivalry between the United States and China has evolved far beyond the realms of hardware, software, or trade. It's now a deeper struggle—one that touches on global leadership, competing ideologies, and the very structure of international power. At the center of this race are emerging technologies like artificial intelligence, quantum computing, surveillance tools, and next-generation telecommunications. These aren't just tools of innovation—they're reshaping military strategies, redefining how governments connect with citizens, manage economies, and project influence on the world stage.

For Pakistan, this rivalry isn't just a distant geopolitical drama—it's a daily reality. As a middle power strategically positioned in Asia, Pakistan finds itself navigating the turbulence of this new tech-fueled competition. On one side, China's deepening role in Pakistan's digital and infrastructure sectors—especially through CPEC—offers significant opportunities for growth and modernization. But it also comes with new forms of dependency and digital exposure. On the other hand, Pakistan's more complex and often uneasy relationship with the United States, particularly in the tech domain, limits its room to maneuver and diversify.

This article has argued that Pakistan's strategic future doesn't lie in simply choosing sides, but in choosing wisely. The country's agency rests in its ability to recognize the risks of alignment and

focus on strengthening its own foundations—through investing in local tech capacity, building resilient institutions, and enacting strong legal and digital safeguards. A non-aligned, thoughtful approach can allow Pakistan to engage with global powers on its own terms.

If Pakistan is to thrive in a world increasingly driven by algorithms and data, it must avoid becoming just another battleground in someone else's digital war. Instead, it must actively shape its own future—where technological choices reflect national priorities, legal protections uphold sovereignty and rights, and innovation grows from within. The question is no longer about choosing between Silicon Valley and Shenzhen. The real task is ensuring that Pakistan's digital destiny is written in its own code.

References

1. Ahmed, Z. (2022, February 23). *Pakistan's deepening tech dependence on China*. The Diplomat. https://thediplomat.com/2022/02/pakistans-deepening-tech-dependence-on-china/
2. Atlantic Council. (2022). *The GeoTech Decade: Pathways to Global Leadership in an Era of Strategic Competition*. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-geo-tech-decade/
3. Carnegie Endowment for International Peace. (2023, April 25). *Pakistan's Digital Security Gap: Bridging the Divide*. https://carnegieendowment.org/2023/04/25/pakistan-s-digital-security-gap-pub-89645
4. Hillman, J. (2021, January 8). *The Digital Silk Road: China's Techno-Geopolitics*. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/digital-silk-road-chinas-techno-geopolitics
5. Khan, S. (2021). *Pakistan's technology governance and data security challenges*. Stockholm International Peace Research Institute. https://www.jstor.org/stable/resrep30516
6. Pauwels, E. (2023). *The Promise and Peril of Digital Non-Alignment*. Egmont Institute. https://www.egmontinstitute.be/the-promise-and-peril-of-digital-non-alignment/
7. Rolland, N. (2020, January 28). *China's Vision for a New World Order*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/01/28/china-s-vision-for-new-world-order-pub-80793
8. Segal, A. (2018, August 14). *When China Rules the Web*. Foreign Affairs. https://www.foreignaffairs.com/articles/2018-08-14/when-china-rules-web
9. Zeng, J. (2021). *The Political Economy of China's Digital Silk Road*. *International Affairs, 97*(4), 1109–1126. https://onlinelibrary.wiley.com/doi/10.1111/1468-2346.13113