How to Cite This Article: Rasheed, E. A. (2025). Cyber Security in International Conflict: US China Cyber Competition and Its Impact on India. *Journal of Social Sciences Review*, 5(2), 156-162. https://doi.org/10.62843/jssr.v5i2.549

Volume 5, **Issue** 2 (Spring 2025)
Pages: 156-162
ISSN (Online): 2789-4428
DOI: 10.62843/jssr.v5i2.549
Corresponding Author: Esha Abdul Rasheed (Email: f2023188047@umt.edu.pk)

JOURNAL OF SOCIAL SCIENCES REVIEW (JSSR)

Cyber Security in International Conflict: US China Cyber Competition and Its Impact on India

Esha Abdul Rasheed [a]

Abstract: *The rising cyber rivalry between China and the United States is the significant part of modern-day global conflict, with far-reaching consequences for global security, economic stability, and geopolitical power balance. The nature of cyber competition between US-China cyber is examined in this paper, with a focus on cyber espionage, digital warfare, and artificial intelligence-powered cyber capabilities. It examines how this rivalry impacts India's national security, technological advancement and diplomatic status in the Indo-Pacific area are affected by this rivalry. Using theories of international relations like as realism and the security dilemma, the paper examines the strategic objectives behind cyber operations and their cascading implications on third-party nations such as India. The findings suggest that, while cyber rivalry exacerbates regional instability, it also forces India to strengthen its cyber defenses and form develop strategic alliances, so thereby shaping its role as a crucial actor in the changing digital geopolitical environment.*

Keywords: US-China Cyber Rivalry, Cyber Warfare, Technological Sovereignty, Cyber Espionage

Introduction

In the twenty-first century, cyberspace has become as a critical front in international conflict, where the states and non-state caring out espionage, sabotage, and influence operations in place of traditional kinetic warfare. The new battlefield is the digital conflict between the United States and China which represents this new arena, in which both nations want technological dominance, economic profit, and military prowess. China's rapid expansion of cyber capabilities, driven by state-sponsored hacker organizations and which is AI-powered digital tools, calls into question the US's long-standing cyber superiority. This rivalry is not limited to the bilateral conflict and its impacts role global international supply lines, essential infrastructure, and third country security calculations, especially those of India.

In the midst of this cyber war, India, which is at the intersection of the Indo-Pacific geopolitical rivalry between the United States and China, presents particular opportunities and challenges. India must manage the dangers of cyber espionage, the possibility of cyberwarfare spreading, and the need to conform to the cyber policies of big nations as a growing digital power with growing cyber infrastructure and strategic interests. The mechanics of the cyberwar between the United States and China are examined in this article, along with its strategic implications for India's foreign and national security.

Research Question

- What are the principal features of the US China cyber rivalry in terms of strategy, capabilities and goals?
- In what ways does cyber competition between the US and China influence India cybersecurity environment and strategic stance?
- What theories of international relations can best explain the behavior of the US China and India in this cyber war?
- How can India effectively respond to the challenges and opportunities arising from the US China cyber competition in an effective manner?

[a] Research Scholar, Department of International Relations, University of Management and Technology, Lahore, Punjab, Pakistan.

Research Answers

Characteristics of US-China Cyber Rivalry

The US-China cyber competition is multidimensional involving espionage, sabotage and the technological supremacy race especially in artificial intelligence, quantum computing and semiconductor technologies. China Made in 2025 strategy prioritize digital sovereignty and AI-pushed governance, aiming to reduce reliance on US technology and assert global leadership. The US nations with programs such as the CHIPS Act and enhanced cyber defense units to protect critical infrastructure and intellectual property.

Chinese cyber activity has grown ever more belligerent and calculating targeting US military networks, government and private sector tech companies. Volt Typhoon and other groups have been accused of planting malware on key infrastructure, marking a transition from traditional espionage to possible precursor to kinetic warfare. The US focuses on deterrence and explicit signaling that cyber attacks will not be unpunished, as both sides invest in AI-powered cyber war capabilities that can drive conflicts quickly out of control.

Impact on India Cybersecurity and Strategy:

- Given its positions as a frontline state in the Indo-Pacific, India is at the risk of increased cybersecurity risk. Increased attacks on its India government networks, keys infrastructure, and its private sectors often them connected to Chinese state-sponsored hackers—are a manifestation of their spillover of US-China cyber wars. Due to its expanding internet user population and the digital economy, India is able to the disruption and espionage.
- The nation should take part in the international cyber governance discussions, develop domestic capabilities, and support its cyber defenses in this order to handle this. Its involvement at Quad (US, Japan, Australia, and India) and other events shows that it is working to create a collective cyber deterrence infrastructure. India's cyber strategy also needs to find a balance between ties with both countries, taking to the advantage of US technology and intelligence cooperation while managing challenging ties with China.
- India's Economy and National Security the cyber competition between the US and China are greatly impacted for India's national security and economy.
- Cyberattacks have the possibility to compromising India's defense capabilities, particularly its to military networks and the strategic assets, which could prevent its ability to respond to foreign threats.
- Cyberattacks on essential business infrastructure, financial institutions, supply chain disruptions, erode investor confidence, and prevent to India's economic development.
- Cyberattacks by the important services can be interrupted on the essential infrastructure, including power, water, and healthcare, endangering public safety and the stability of society.
- China's cyber policy combines actual military operations with the digital espionage, posing a threat to India that requires a complete response. To address these problems, India has a shifted to integrated cyber and the military strategy, as evidenced by initiatives like "Operation Sindoor.”
- Technology and supply chain risks the China-US trade war has an impacts global supply chains, including semiconductors and rare earth minerals that are critical to India’s technology industry. India is facing supply shortages and price hikes but also has chances to develop indigenous capabilities in design of the chip and the rare earth production.

Applicable International Relations Theories:

Realism: survival and power are top states gives priority. The United States and China between the cyber competition reveals power struggle in a new area, with the cyber operations used for the strategic to the advantage and deterrence.

Dilemma Security: States develop the offensive and defensive weapons in this response to the insecurity created by cyber capabilities it increases the danger of the escalation and make people mistrust of one another. Perceived the Chinese threats and a desire to align with the US security standards are two factors contributing to India's cyber buildup.

Complex Interdependence: Economic links while improving security. The US and China's economic and the technological interdependence complicates to the conflict, affecting India's strategic calculus to keep up.

India Effective Responses

- Strengthen cyber infrastructure resilience and invest in AI-driven cybersecurity technologies.
- Improve intelligence cooperation among allies, including those in the Quad and the US.
- Encourage international conventions and agreements to avoid escalation risks in cyber conflicts.
- Create local semiconductor and AI companies to lessen reliance on technology.
- Achieve strategic autonomy by balancing relations with both the US and China.

Theoretical application: International Relations and Cybersecurity

The US-China cyber rivalry and its influence on India are the best understood through the Realism and Security Dilemma frameworks. Realism claims that government under an anarchic international system, governments prioritize survival and power optimization, resulting in the competition in various field, including cyberspace. Both the United States and the China see cyber capabilities as their important for the military advantage and the economic security, resulting in an arms race in cyber weapons and the defenses. The security problem develops when each side's cyber buildup to the makes the other feel in endangered, causing more escalation. India, recognizing this rivalry, responds by strengthening its own cyber capabilities in order to prevent exposure, thereby prolonging the cycle. However, characteristics of complex interdependence apply as the connection in economy and technological exchanges between the major nations generate to incentives for restraint cooperation in a specific cyber governance of areas.

Theoretical Application of Deterrence Theory in International Relations and Cybersecurity

Deterrence theory, which was first created during the Cold War to the prevent nuclear war, is based on the notion that a state can prevent an enemy from conducting an invasion through the issuance of credible threats of retaliation or making attacks ineffective. However, this theory presents unique challenges in the context of cyber security, it is nevertheless an essential resource for understanding state conduct and strategic competition.

Rational actors stay clear of conflict when the expected expenses surpass the advantages, according to deterrence theory. It is composed of two primary parts:

Deterrence by Punishment: involves vowing to keep revenge that would be expensive for the attacker an unacceptable amount of money.

Defending against: attacks by making them ineffective or too much expensive is known as deterrence by denial. For the deterrence of work, this threat needs to be real, expressed the accurately, and the enemy needs to the logical enough to understand that consequences.

Applying the Theory of Deterrence to Cybersecurity

Difficulties in Cyberspace Issues: In opposed to traditional warfare, it is challenging to determine with certainty the source of a cyberattack, making the reaction more challenging.
Asymmetric abilities: State and non-state it takes extremely little money for organization to launch cyberattacks. Cyberattacks can occur goal a variety of multiple system at once.
Conflicting Intent: Because cyber activities can be very from the sabotage to espionage, it can be difficult to determine if an answer is suitable.
International Norms: Promoting cyber agreements and norms to set expectations of state behavior and lower conflict risk.

Offensive Realism

According to offensive realism, states to seek optimize their security and power by the developing offensive abilities. The China and US are improving their AI and cyber offensive tools to gain strategic advantage.

Consequently, India, needs to support its own cyber power to the maintain security and its important influence in the region.

Chinese Cyberattacks on India Vital Infrastructure

By China accused of targeting Indian grids of power and the network communication in 2020 Ladakh border tensions. This offensive action is reliable with the offensive realism. It maintain that governments to seeks degrade adversaries in order to weaken enemies and improve their own security.

Cybersecurity Policy Shifts

India’s latest actions to strengthen in cyber defense and offense, including establishing cyber structures of commands, represent a change in logical of power towards offensive realism’s reality the maximize of power logic in cyberspace.

Stuxnet as an Example of a Cyber offensive Plan

India was not directly involved in the US-Israel Stuxnet cyberattack on Iran's nuclear program. However, it does show an important concept in offensive realism: that powerful nations can use cyberweapons in an offensive manner to undermine the strategic capabilities of their enemies.

Information Warfare and Influence Operations

- Cyber rivalry involves more than simply hacking but it also involves and influencing public opinion and controlling narratives.
- China claimed to the cyber-enabled disinformation advertisements in the US and neighboring countries reflect offensive realism’s idea of weakening the unity and authority of competitions.
- In response, the US intensifies the competition by the launching its own cyber influence activities.

Cyber Power as a Means to Regional Hegemony

- China is expanding its cyber influence throughout Asia and Africa through the Digital Silk Road, a digital infrastructure initiative part of the Belt and Road Initiative (BRI).
- According to offensive realism, China subtly challenges US influence by using cyber power aggressively to increase its regional domination.

Impact on India: Additional Perspective

India as a Cyber Battleground: The political, military, and the infrastructure sectors of India are the targets of cyberattacks that are allegedly coming from China. According to offensive realism, in order to the dissuade enemies and to establishment itself as a regional power, India must not only defend its cyberspace but also create offensive tools.

Positioning vs Strategic Autonomy: Offensive realism concept of the enhancing power without becoming overly to dependent is seen in India delicate balancing to the act between US cyber assistance and the preserving strategic autonomy. Through its investments in the strategic alliances and the domestic cyber capabilities, India's cyber policy is becoming to more and more offensively realistic.

Cyber Norms and Diplomacy: Global developments take part in the India of cyber criteria in order to the influence laws that support its security objectives. This is explained by offensive realism as a formalization attempt power in advantages and limits the cyberactivity of the rivalry.

Game theory

In cybersecurity, the strategic relationship between attackers and the defenders is game as a modeled in which every party to makes the decisions to maximize their personal gain while dealing with uncertainty.

Strategies: The primary participants are attackers (e.g., state-paid hackers from China and US) and the India defenders cyber defense agencies. Defenders decide how too much resources to devote to defense and the retaliation, although attackers decide either or not to the attack.

Defense Attack Games: Cybersecurity can be thought of as a repeating game in which defenders try to make repairs or reduce weakness while attackers attempt to exploit them. When no party can one-sidedly after their strategy to increase their payout the balance stable state occurs.

Examples

- Plan India's defensive or the diplomatic India can select how to divide up its limited cyber protection resources among its important infrastructure by applying game theory.
- Determine when a cyberattack is most likely to occur and plan your defenses properly.
- Response to increasing situations in China-US cyberwarfare.

India’s Response and Future Outlook

India is aggressively strengthening its cybersecurity strengthening stance by making more investments, policy changes, and the international cooperation. The government and commercial sector's attempts to fight changing the risks are expected to drive for a major growth in the India's cybersecurity market.

India’s collaboration with the US and Quad associates supply chain security, on the cyber norms, and new emerging technologies is essential for building a strong cyber ecosystem. Moreover, India’s concentrate on AI-driven cybersecurity tools seeks to stay up with the advanced strategies used by enemies.

Nevertheless, challenges stay put. Contribution difficulties, quick technological changes, and the long boundaries between cybercrime, espionage, and the warfare making thing more difficult India’s response. Keeping the strategic independence while lining up with major powers of the cyber policies will be essential to India’s success in inside the domain.

Conclusion

The ongoing cyber competition between the United States and China is one of the most important aspects of modern international warfare, changing global power relations and security systems. This competition is more than just a bilateral battle; it resonates across regions, therefore impacting nations like the strategic environment of countries such as India. As a developing state located at the Asia's crossroads, India is both a target and a key factor in the evolving cyber warfare scene as a raising nation. The cyber competition between the US and China has significant consequences for India, including national security, economic stability, diplomatic ties, and technical sovereignty and the national security.

Increased Cyber Threats Against India

India's critical infrastructure, defense facilities, and expanding technology sectors have come under increased attack from China's cyber strategy, which includes the aggressive espionage, intellectual the theft of property, and disruptive cyber operations. This aligns with the China's broader geopolitical objective to the establish its regional supremacy and counterbalance the might of the US and its allies, especially India. The strategic intent behind these actions is the evident from Chinese cyberattacks that have attacked Indian military communication networks, power grids, and even to vaccine manufacturing, especially during the COVID-19 pandemic. Frequent cyberattacks highlight India's vulnerability and the requirement for strong cyber security protocols.

Strategic Realignment and Enhanced US-India cyber Cooperation

The rising cyber conflict has the triggered a strategic realignment, bringing India closer to the United States. Enhanced defense collaboration, as seen by the agreements like the Basic Exchange and collaboration Agreement (BECA), has given India access to the advanced geospatial intelligence and cyber security technologies. This relationship increases to India's ability to detect, deter, and respond to cyberattacks emanating from China, contributing to a more resilient national security posture. The US-India partnership goes beyond military areas to include collaborative cyber exercises, intelligence sharing, and capacity construction, which improve India's cyber defenses.

The Challenges of Technological Dependency and Economic Weaknesses

Due to its economic and technological reliance on China, India faces challenging its context when it comes to security cooperation with the US. India's biggest supplier of consumer technology goods and essential electrical components is still China. Due to this economic interdependence, India's technological environment is vulnerable to both cyberattacks and Chinese influence, creating a dual-use dilemma. China can exert pressure on India through economic coercion or cyber sabotage, which is made worse by the US-China cyber battle. India's efforts to this promote domestic internet infrastructure and outlaw Chinese tech companies like Huawei are measured steps to reduce dependency and its increase technological sovereignty.

India's reaction to the cyber war between the United States and China will able to impact not just its own security path but also the broader Asian geopolitical order. India may use this challenge as an opportunity to become a crucial cyber power by proactively strengthening its cyber defenses, developing its technological environment, and actively to engaging in global cyber governance. India's sovereignty would strengthened to the regional stability would be promoted, and the internet norms and regulations would be shaped for the twenty-first century.

References

Ali, S. A & Amin, F. (2025) Comparative Study of US-China Cyber Strategy and Its Impact on the Indo-Pacific Region. *Qlantic Journal of Social Sciences and Humanities*, 6(2), 144-157 https://doi.org/10.55737/qjssh.vi-ii.25351

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/

Cheng, D. (2025, June 18). *The Element of Surprise: Space and Cyber Warfare in U.S.-China Rivalry*. United States Institute of Peace. https://www.usip.org/publications/2025/06/element-surprise-space-and-cyber-warfare-us-china-rivalry

Sardar Jahanzaib Ghalib. (2025, April 26). *Issue Brief on "The U.S.-China AI and Digitalization Race: Geopolitical Implications and Strategic Trajectories" | Institute of Strategic Studies Islamabad*. Issi.org.pk. https://issi.org.pk/issue-brief-on-the-u-s-china-ai-and-digitalization-race-geopolitical-implications-and-strategic-trajectories/

Singh, N. K. (2025). *China's Cyber Maze: Challenges and Prospects for the United States - Australian Institute of International Affairs*. Internationalaffairs.org.au. https://www.internationalaffairs.org.au/australianoutlook/chinas-cyber-maze-challenges-and-prospects-for-the-united-states/