Wah Academia Journal of Social Sciences
Volume 4, Issue 1, Jun 2025, pp. 1360-1379
ISSN – E 2958-8731 P 2958-8723

India Pakistan cyber skirmishes and Afghan digital infrastructure: A realist analysis of cross-border cyber spillovers in post –Taliban Afghanistan

Muhammad Mudeer[1]

Abstract

This paper looks at how cyber operations between India and Pakistan negatively impact cross –border data flows telecommunications network and Afghanistan's delicate digital infrastructure, especially after the Taliban took back control in August 2021. This study examines how bilateral cyberwarfare affects Afghanistan's delicate digital environment using classical realism as the theoretical foundation and specifically referencing the writings of Hans Morgenthau and Kenneth Waltz. From August 2021 to May 2025, the study used a qualitative technique that included expert interviews, case study analysis, and documents analysis according to research India Pakistan cyberwarfare causes serious collateral damage to Afghanistan's digital infrastructure, posing a challenging security situation for the Taliban regime. The study shows that Afghanistan's geographic.it is especially vulnerable to cyber crossfire due to its position and technology reliance, and these vulnerabilities are made worse by the Taliban's poor ability to govern. The deliberate disruption of Afghan telecommunications networks, hacked cross-border data transfers and Indians and Pakistanis weaponization of digital infrastructure are some of the main conclusions. The study comes to the conclusion that regional cyberwarfare has seriously undermined Afghanistan's digital sovereignty, with consequences for the provision of humanitarian help, economic recovery, and the stability of governance. Based on realism principles, this study offers policy proposals that include creating neutral digital corridors, broadening technology alliances, establishing cyber non-interference agreements.

Keywords: Afghanistan digital infrastructure India Pakistan cyber conflict, Taliban governance, cross-border cyber operations, south Asian cybersecurity, digital sovereignty, cyber spillovers, Regional cyber warfare

[1] Department of Political Science & International Relations, University of Management and Technology, Lahore – Pakistan

CC BY

Introduction

An important turning point in South Asia geopolitics was the Taliban's resurgence in Afghanistan in August 2021, which increased cybersecurity vulnerabilities in the region. Already vulnerable due to decades of violence, Afghanistan's digital infrastructure today confronts hitherto unheard-of difficulties as a result of the cyberwarfare between India and Pakistan (Johnson &Ahmed, 2022). The nation is especially vulnerable to the collateral harm of bilateral cyber operations between its neighbors due to its key geographic location at a digital crossroads between south and central Asia India -Pakistan cyber activities have unintentionally turned Afghanistan's digital infrastructure _which includes internet service providers, telecommunications networks, and cross-border data channels into a battlefield. In his examination of Pakistan cybersecurity predicament, Hamza (2025) shows how the nation's location between powerful cyber nations produces special vulnerabilities that impact regional stability in addition to bilateral disputes. These vulnerabilities have been made worse by the Taliban's poor technical capabilities and international isolation, which has resulted in a complex security environment where external cyber activity threatens Afghanistan's digital sovereignty. Tow important research questions are addressed in this study: why does Afghanistan's neutral position make its digital infrastructure susceptible to cyberwarfare between India and Pakistan? and what particular effects do India-Pakistan bilateral cyber operations have on Afghanistan's digital governance capabilities, cross-border data flows, and telecommunications networks under Taliban rule? These enquiries are crucial to comprehending the difficulties of preserving digital sovereignty in disputed geopolitical contexts as well as the wider effects of regional cyberwarfare on weak governments.

Beyond Afghanistan's boundaries, this research is important because it sheds light on how cyberwarfare between superpowers can weaken the digital infrastructure of states that are adjacent. Because of its technical isolation and lack of international legitimacy, the Taliban's governance model offers a unique case study for analyzing how non –state actors manage the spillovers effects of regional conflicts while navigating complicated cyber environments.

Review of the Literature

- **Cyber conflict and regional spillovers**

CC BY

The significance of collateral damage and spillover effects in regional cyber operations has been acknowledged more and more in the scholarly literature on cyber conflicts. Rid (2013) lays the groundwork for comprehending how cyber actions cross conventional lines and have unforeseen repercussions for nearby states. This work is especially pertinent to comprehending how India-Pakistan cyber conflicts is offered by Valeriano and Maness (2015), who highlight how regional powers projects power influence through cyber capabilities. Despite Afghanistan's little direct engagement in bilateral issues, their work on cyber coercion helps explain why the country's digital infrastructure becomes a target for both India and Pakistan cyber activities.

According to sanger (2018), cyber operations are becoming a crucial part of great power struggle, putting smaller states that are sandwiched between major powers at risk in new ways. Comprehension Afghanistan's place in the India –Pakistan cyber dynamic and the difficulties of preserving digital neutrality in a divisive regional setting require a comprehension of this analysis.

- **Afghanistan's digital infrastructure and Governance Challenges**

The developmental features of internet penetration and telecommunications expansion have been the main focus of scholarly work on Afghanistan's telecom industry under Taliban control is given by bjelica and rutting (2023), who emphasize the difficulties in preserving digital connectivity while dealing with international sanctions and technological isolation.

The country's digital infrastructure risks, such as outdated equipment, a lack of technical capability, and reliance of foreign technology providers, are through examined in the world bank's digital Afghanistan Report (2022). the foundation for comprehending how Afghanistan is especially vulnerable to external cyber operations due to its digital vulnerabilities is established by this work.

The conflict between enforcing ideological controls over digital information and preserving connectivity for economic reason is highlighted in Foschini's (2024) analysis of the Taliban's approach to digital government. understanding how governance issues increase Afghanistan's susceptibility to cyber spillovers requires this analysis.

CC BY

- **India-Pakistan Cyber Dynamics and Regional Impact**

Since the Galwan valley incident and the ensuing cyber escalations, there has been a notable increase in the body of literature on the cyber conflict between India and Pakistan.in the context of the India –China cyberwar, Hamza (2025) offers vital insight into Pakistan cybersecurity predicament and shows how intermediate powers manage their interactions with great powers while navigating difficult cyber settings.

Understanding how Afghanistan has comparable difficulties in controlling the fallout from regional digital infrastructure in addition to bilateral targets. Their research on telecommunication disruption and cross-border data manipulation provides crucial background information for comprehending the processes influencing Afghanistan's digital infrastructure.

Regardless of their participation in bilateral disputes, neighboring nations are impacted by the systemic vulnerabilities created by regional cyber wars, according to the Carnegie India report on South Asian Cybersecurity (2024). This insight is essential to comprehending why, in spite of Afghanistan's poor cyber capabilities, its digital infrastructure is targeted.

Theoretical Framework

In order to comprehend Afghanistan's place in the India-Pakistan cyber dynamic, this study uses classical realism as its main theoretical framework, notably referencing the writings of Hans Morgenthau (1948) and Kenneth waltz (1979).this study adopts realism principles to investigate how Afghanistan's unique situation as a weak state between big cyber power's produces unique vulnerabilities and problems, building on hamza's (2025) application of realist theory of Pakistan's cybersecurity dilemma.

- **Core Realist Assumptions in the Cyber Domain**

A strong framework for comprehending Afghanistan's cyber vulnerabilities is provided by classical realism's emphasis on power relation and state behavior in anarchic contexts. Stronger governments might strategically take advantage of the digital infrastructure of their weaker neighbors in the cyber domain due to the lack of efficient international governance mechanisms (Waltz,1979). Afghanistan's situation is a prime example of this dynamic since it is unable to withstand the

CC BY

spillover effects of India-Pakistan cyber activities due to its low cyber capabilities and international isolation.

In order to comprehend cyber dynamic, s the realist focus on power as the main medium of exchange in international relations is especially crucial. According to Hamza (2025) Cyber capabilities are new form of power that may be used to disrupt of the economy, obtain intelligence, and accomplish political objectives. Due to Afghanistan's inferior cyber capabilities compared to India to Pakistan, both nations have weakness that they can take advantage of for strategic positioning, influence operations, and intelligence collection.

- **Security Dilemma in Multi-State Cyber Environments**

Afghanistan's cyber environment is a unique manifestation of the security dilemma notion, which is central to realism theory. Afghanistan confronts a triangle security problem in which attempts to bolster its cyber defenses or align with either India or Pakistan is viewed as threats by the other party, in contrast to the bilateral security issue that Hamza (2025) outlined in the context of Pakistan. Afghanistan's security measures may unintentionally increase regional tensions due to this complex dynamic.

Afghanistan's reliance on technology adds to the complexities of the security challenge. The nation's dependence on foreign technology suppliers, like as businesses from Pakistan and India, leaves it vulnerable to attacks from either side. Afghanistan's technological decisions have geopolitical ramifications that go beyond technical reasons, much like Pakistan's predicament with Chinese technology integration (Hamza, 2025).

- Weak state Dynamics and Cyber Vulnerability

The way weak states are treated in realist theory offers crucial insights regarding Afghanistan's cyber vulnerability. Afghanistan is unable to control cyber threats or negotiate cyber agreements with regional countries due to the Taliban government's weak technological capabilities and lack of international recognition. The nation's reliance on foreign technical know-how and equipment exacerbates this weakness and leaves it open to outside influence and control.

Afghanistan's cyber environment, where both India and Pakistan can operate with little responsibility due to a lack of efficient governance systems, is a prime example

CC BY

of the anarchic nature of the international system. According to Hamza (2025), "cybersecurity is essentially a self-help activity" in anarchic settings; yet, Afghanistan is especially susceptible to external exploitation due to its weak potential for self-help.

Methodology

This study uses a qualitative research methodology that combines expert interviews, case study analysis, and document analysis to investigate how India-Pakistan cyberwarfare has affected Afghanistan's digital infrastructure. The study design adheres to accepted qualitative research guidelines that have been modified for cybersecurity research settings by Creswell (2018).

- **Data Collection Methods**

Official Taliban government statements on telecom policy, technical reports from Afghanistan's telecom regulating body, and diplomatic correspondence about cyber events are examples of primary sources. The Afghan government's viewpoint on cyber issues and policy solutions is directly revealed by these sources.

Secondary sources include technical evaluations of Afghanistan's digital infrastructure, reports from global cybersecurity firms, and scholarly analysis of regional cyberwarfare. Reports from companies like Kaspersky, FireEye, and local cybersecurity research institutes are important sources. This study uses "media analysis, cybersecurity industry reports from organizations like Recorded Future and CyFirma" in accordance with Hamza's (2025) methodology in order to offer a contextual understanding of regional cyber dynamics.

Telecommunications engineers, cybersecurity specialists, and regional security analysts with knowledge of Afghanistan's digital infrastructure issues participated in expert interviews. The usefulness of present mitigating techniques and the real-world ramifications of cyber spillovers are both qualitatively revealed by these interviews.

- **Analytical Framework**

To find trends in cyber incidents and their effects on Afghanistan's digital infrastructure, the study uses theme analysis. In accordance with Hamza's (2025) methodology, the analysis centers on "cyber incidents that occurred from" August

CC BY

2021 to May 2025, encompassing the time frame of Taliban rule and the intensifying cyber operations between India and Pakistan.

Case study analysis looks at particular instances where cyber operations between India and Pakistan had a direct impact on Afghanistan's digital infrastructure, such as cross-border network intrusions, data flow disruptions, and telecommunications outages. The realist theoretical framework is applied to each case study in order to comprehend the strategic reasons and consequences of cyber spillovers.

Limitations and Ethical Considerations

The report admits a number of methodological flaws, such as the sensitive nature of cybersecurity data, limited collaboration from certain international organizations because of Taliban governance, and restricted access to classified government records. The research must negotiate "the anarchic structure of the international system," where security concerns restrict information sharing, much to the difficulties mentioned by Hamza (2025).

Protecting interview subjects' confidentiality, avoiding sharing critical technical data that would jeopardize Afghanistan's cyber defenses, and making sure that study results don't unintentionally give hostile actors tactical intelligence are all examples of ethical considerations.

Analysis and Findings

- **Afghanistan's Digital Infrastructure Vulnerabilities**

The intricate web of weaknesses in Afghanistan's digital infrastructure makes it especially vulnerable to the repercussions of cyber operations between India and Pakistan. Due to its heavy reliance on foreign technology and experience, the nation's telecommunications network, which was substantially reconstructed between 2001 and 2021, has several potential weak points.

The main components of the telecommunications infrastructure include mobile networks run by Roshan, Etisalat, and MTN Afghanistan, as well as a few fixed-line services and internet access. These networks are susceptible to disruption from regional cyber warfare since they rely on cross-border data links via Pakistan, Iran,

CC BY

and Central Asian nations (Afghanistan Telecommunications Regulatory Authority, 2023).

Afghanistan's "limited national cybersecurity skills, strategic dependencies, and relatively new digital infrastructure make it vulnerable to direct attacks and collateral damage from" regional cyber operations, much like Pakistan's predicament, as outlined by Hamza (2025). These weaknesses have been made worse by the Taliban government's limited technical capability and international isolation, which have made it easier for outside players to operate without worrying about being discovered or retaliated against.

- **Timeline of Cyber Incidents and Impact Assessment**

August 2021: After the Taliban regained control, there was a sharp rise in cyberattacks on Afghanistan's digital infrastructure by Pakistan and India. While Pakistani players attempted to get continuous access to Afghan government computers, Indian intelligence agencies conducted reconnaissance operations against Taliban communication networks (Cyber Intelligence Report, 2021).

November 2021: As India-Pakistan cyberwarfare intensified, Afghanistan's international internet connectivity was severely disrupted. While Indian cyber operations interrupted data cables between Pakistan and Afghanistan, creating significant internet disruptions that impacted humanitarian operations, Pakistani hackers targeted Indian-owned telecoms equipment in Afghanistan (Digital Frontier Foundation, 2021).

March 2022: In order to obtain intelligence on Taliban communications and track cross-border insurgent activity, Indian cyber troops launched the "Operation Digital Crossroads" campaign, which targeted Afghanistan's telecom switching centers. Banking, healthcare, and emergency services were all negatively impacted by this operation's unintentional disruption of civilian telecommunications systems (South Asian Cyber Watch, 2022).

In order to provide ongoing monitoring capabilities and thwart possible Indian intelligence operations, Pakistani cyber actors initiated "Operation Silk Route," which targeted Afghanistan's eastern telecommunications infrastructure, in June 2022. The operation hacked multiple government communication systems and seriously damaged civilian networks (Regional Security Monitor, 2022).

CC BY

September 2023: The "Kabul Network Infiltration" incident sparked a cyberwar within Afghan digital infrastructure when Indian and Pakistani hackers targeted Afghanistan's main communications hub at the same time. The event demonstrated how bilateral cyber activities had turned Afghanistan's networks into a battlefield (Afghanistan Digital Security Report, 2023).

January 2024: Trade, remittances, and the coordination of humanitarian supplies were all impacted by the selective blocking of data transmission through Afghanistan that both India and Pakistan deployed, which worsened cross-border data flow difficulties. Beyond conventional security goals, these disruptions showed how cyber operations could accomplish political and economic goals (Economic Impact Assessment, 2024).

The next escalation occurred in May 2025 and featured coordinated attacks on the digital infrastructure of Afghanistan's financial sector. Indian and Pakistani actors targeted banking networks in an effort to obtain intelligence and impede money flows. This event demonstrated the growing extent of cyber spillovers to vital economic infrastructure outside of telecommunications (Financial Cyber Security Alert, 2025).

Realist Analysis of Strategic Motivations

Realistically speaking, Afghanistan's digital infrastructure is seen by both India and Pakistan as a strategic resource that may be used for influence operations, intelligence collection, and strategic placement. Hamza (2025) said that "cyberwarfare crosses technological boundaries and becomes an economic struggle," and the escalation pattern reflects this, with both nations exploiting Afghanistan's digital vulnerabilities to further their larger strategic goals.

Monitoring cross-border terrorist activity, obtaining information on Pakistan-Taliban collaboration, and preserving influence in an area where it has no physical presence are all strategic goals of India's cyber operations in Afghanistan. Despite its diminished military and diplomatic presence, India is still able to sustain intelligence capabilities by utilizing Afghanistan's digital infrastructure.

Pakistan's strategic objective in preserving influence over its neighbor while thwarting Indian intelligence operations is reflected in its cyber operations in

Afghanistan. In line with Hamza's (2025) description of strategic hedging, Pakistan's cyber operations in Afghanistan are an attempt to "maintain flexibility in relationship with both regional powers to maximize security.

Impact on Cross-Border Data Flows

One of the biggest effects of the cyberwarfare between India and Pakistan on Afghanistan's digital infrastructure is the disruption of cross-border data transfers. Afghanistan's economy, which is already precarious under Taliban administration, is largely dependent on internet links for coordination of humanitarian aid, trade, and remittances.

Due to the implementation of selective blocking and data traffic monitoring in both countries, cross-border data flows through Pakistan have been especially impacted. Due to frequent disruptions in digital payment networks, communication platforms, and logistical coordination systems, Afghan enterprises involved in international commerce now face significant obstacles (International commerce Digital Infrastructure Report, 2024).

Given that international aid agencies mostly rely on digital communications and data transfers to coordinate relief efforts, the humanitarian ramifications are especially dire. Aid delivery has been directly hampered by disruptions to these systems. Emergency response skills and assistance for refugees (UN Digital Humanitarian Response, 2024).

Taliban Governance and Cyber Response Capacity

restricted technical capability, international isolation, and conflicting agendas have restricted the Taliban government's ability to respond to cyber spillovers. The Taliban lacks the institutional structure and technological know-how necessary to handle sophisticated cyberthreats, in contrast to more established governments with sophisticated cyber response capabilities.

The predicament of the Taliban is indicative of larger issues that weak regimes face in cyberspace, where "cybersecurity is essentially a self-help activity" but the ability to assist oneself is severely constrained (Hamza, 2025). International sanctions, restricted access to cutting-edge cybersecurity technologies, and a lack of

collaborative links with key cyber powers have all hindered the government's efforts to address cyber vulnerabilities.

Since attempts to censor internet material and limit digital liberties have weakened the technological foundation required for efficient cyber defense, the Taliban's ideological approach to digital governance has added to the complexity. As a result, there is now a paradox whereby security measures intended to safeguard the regime have made it more susceptible to outside cyberattacks (Taliban Digital Policy Analysis, 2024).

Discussion and Implications

- **Strategic Implications for Regional Stability**

Afghanistan's digital infrastructure is being impacted by India-Pakistan cyberwarfare, which has wider ramifications for regional security and stability. According to Hamza's (2025) assessment that "cybersecurity has become deeply connected to traditional geopolitical processes," Afghanistan's experience shows that neighboring states might become unstable due to cyber wars even if they are not directly involved in bilateral disputes.

India-Pakistan cyber operations using Afghanistan's digital infrastructure as a battlefield set the stage for future confrontations of a similar nature in other areas. The stability of digital infrastructure worldwide is at risk due to the normalization of cyber spillovers as permissible collateral damage in bilateral conflicts, especially in areas with inadequate governance and weak cyber defense capabilities.

Hamza (2025) noted that "regional cyber infrastructure is interconnected, attacks that target one nation frequently affect its neighbors, posing a risk that extends beyond bilateral ties." These regional security implications are consistent with this finding. The history of Afghanistan serves as an example of how powerful nations can take advantage of this interconnection to further their strategic goals at the expense of their less powerful neighbors.

- **Humanitarian and Economic Consequences**

Cyber spillovers have long-term effects on stability and development in addition to short-term technical problems. Disruptions to digital commerce, international

CC BY

banking, and telecommunications systems that are necessary for commercial operations have severely undermined Afghanistan's already precarious economy.
Given that international organizations mainly rely on digital networks for funding transfers, logistics, and coordination, the impact on the delivery of humanitarian relief has been especially severe. Delivering food aid, medical supplies, and emergency relief to vulnerable populations has been directly impacted by cyber disruptions (Humanitarian Digital Infrastructure Report, 2024).

Due to their reliance on digital connectivity for service delivery, coordination, and access to global resources, healthcare and education services have also been greatly impacted. The long-term effects of these services' interruption on Afghanistan's social stability and human development (Social Services Digital Impact Assessment, 2024).

- **Lessons for Middle Powers and Weak States**

Other nations dealing with comparable issues from regional cyberwarfare can learn a lot from Afghanistan's experience. Hamza's (2025) appraisal of Pakistan's situation between India and China is echoed by this example, which shows how weak states get "caught in the crossfire" of large power cyber activities.
Afghanistan's experience highlights the significance of strategic diversity in digital infrastructure. Countries that rely significantly on a single technology supplier or data channel are more susceptible to political manipulation and cyber spillovers. Creating several redundant digital routes can offer some defense against certain disturbances.

Hamza's (2025) conclusion that "structural challenges that are difficult to address with policy changes alone, such as geographic vulnerabilities, lack of resources, and technical dependence, limit" strategic autonomy in cyber affairs is supported by Afghanistan's experience, which highlights the limitations of defensive approaches alone.

Implications for International Cyber Governance

Significant inadequacies in international cyber governance and the need for new frameworks to shield weak governments from cyber spillovers are highlighted by Afghanistan's experience. Afghanistan and other nations that are collateral damage

in bilateral cyberwarfare are not adequately protected by the current international legal framework.

Preventing the normalization of collateral damage in cyber operations requires the creation of international standards pertaining to cyber spillovers and the defense of neutral digital infrastructure. This calls for fresh strategies for global collaboration that can continue to work even in the absence of official diplomatic ties with disputed regimes.

Given the predicament of weak governments like Afghanistan that are unable to rely on bilateral agreements or regional alliances for cyber defense, the necessity of the international institution for cyber protection mentioned by Hamza (2025) becomes even more urgent.

Proposed Solutions and Recommendations

- **Establishment of Digital Neutrality Corridors**

This paper suggests creating "Digital Neutrality Corridors" to shield Afghanistan's vital digital infrastructure from the consequences of regional cyberwarfare, based on realism ideas of strategic necessity and mutual benefit. These corridors would serve as secure routes for vital digital communications and data flows, just like humanitarian corridors do in conventional battles.

The corridors would be implemented in spite of the Taliban government's lack of international recognition since they would be created through technical agreements between telecom companies rather than official diplomatic accords. In accordance with the suggestion made by Hamza (2025) for "strategic diversification of cybersecurity partnerships," these corridors would incorporate a number of technology suppliers in order to lessen reliance on any one party.

The creation of specialized network infrastructure for vital services including the coordination of humanitarian relief, medical communications, and fundamental financial activities would be necessary for implementation. These networks would be protected from cyberattacks and monitored technically to make sure they aren't being exploited for military or intelligence activities.

- **Neutral Digital Infrastructure Development**

Building neutral digital infrastructure that can operate without interference from regional cyberwarfare should be Afghanistan's top priority. This entails setting up local internet exchange points, domestic data centers, and redundant international connectivity across several nations.

International support is necessary for the development of neutral infrastructure, and this support can be given through technical help as opposed to formal diplomatic agreements. In line with Hamza's (2025) call for "indigenous capacity building," Afghanistan must create indigenous technical capabilities capable of autonomously maintaining and running vital digital infrastructure.

Systems for humanitarian communications, education, and healthcare that can function on separate networks as needed should be prioritized. When regional circumstances allowed, this strategy would enable greater digital connectivity while safeguarding critical services.

- **Cyber Non-Interference Agreements**

Some protection against spillover effects may be offered by the informal cyber non-interference agreements that India and Pakistan have established with regard to Afghanistan's digital infrastructure. Despite wider international tensions, these agreements would be more achievable since they would concentrate on technical rather than political issues.

Based on Hamza's (2025) examination of "regional cyber diplomacy and confidence-building measures," these accords might incorporate clauses pertaining to the exchange of information about common dangers, technical collaboration on regional cybersecurity issues, and procedures for preventing collateral harm to neutral infrastructure.

In order to facilitate cooperation even during times of increased political stress, the agreements would have to be implemented through technical channels as opposed to formal diplomatic ones. This method acknowledges the realist idea that, with the right framework, collaboration can advance state objectives.

CC BY

❖ **International Monitoring and Support Mechanisms**

In addition to fostering international support for the concepts of digital neutrality, the implementation of international monitoring mechanisms for Afghanistan's digital infrastructure may offer some defense against cyber spillovers. All parties would find these processes more acceptable because they would concentrate on technical monitoring rather than political inspection.

Technical aid programs that steer clear of direct political contact with the Taliban regime could be used to provide international help for the development of Afghanistan's digital infrastructure. This strategy keeps political distance from contentious governing structures while allowing for humanitarian and developmental assistance.

In line with Hamza's (2025) suggestion that "European Union nations, especially those with significant cybersecurity capabilities but few geopolitical disputes," should be engaged, Afghanistan could gain technical support from nations that are politically neutral and can offer cybersecurity expertise.

❖ **Strategies for Increasing Regional Confidence**

The impact of cyber spillovers on Afghanistan and other regional nations may be lessened with the creation of regional confidence-building initiatives that are especially aimed at safeguarding civilian digital infrastructure. Instead of emphasizing more extensive political agreements, these initiatives would concentrate on technical collaboration and common security concerns.
In line with Hamza's (2025) plan for a "South Asian Cyber Security Dialogue," regional talks might center on information exchange on common dangers, technical collaboration, and the development of regional cyber standards that are advantageous to all parties.

Cooperation would be possible even during times of political unrest if the measures were to be carried out through commercial and technical channels as opposed to formal diplomatic ones. This strategy acknowledges that even in situations when there are tensions in broader political connections, technological cooperation can benefit both parties.

CC BY

Conclusion

This study has looked at how cyberwarfare between India and Pakistan poses serious risks to Afghanistan's digital infrastructure, highlighting the difficult situations weak governments face when they are entangled in great power cyberwarfare. According to the report, Afghanistan is especially vulnerable to cyber spillovers due to a confluence of factors, including its geographic location, technical reliance, and weak governance under Taliban leadership.

According to the study, "cybersecurity has become deeply connected to traditional geopolitical processes," as noted by Hamza in 2025. Afghanistan's experience demonstrates how these ties can destabilize neighboring governments even if they are not directly involved in bilateral disputes. The results show that major power cyberwarfare affects regional stability and humanitarian conditions, posing systemic concerns that go well beyond the direct players.

Afghanistan's strategic geographic location as a digital crossroads, its technological reliance on foreign providers with conflicting loyalties, the Taliban government's limited cyber defense capabilities, and the lack of effective international protection mechanisms for neutral digital infrastructure are the main conclusions of the study that explain why Afghanistan's digital infrastructure is susceptible to India-Pakistan cyber skirmishes.

According to the study, there are a number of important processes via which bilateral cyber operations affect Afghanistan's digital systems: (4) the weaponization of technological dependencies to accomplish strategic goals; (2) collateral damage from operations targeting the assets of neighboring countries; (3) disruption of cross-border data flows through selective blocking and monitoring; and (5) direct targeting of telecommunications infrastructure for intelligence gathering.

Hamza (2025) concluded that "technological interdependence creates new type of vulnerabilities while traditional security issues continue to exist," and the study's findings support this conclusion. Afghanistan's experience serves as a clear illustration of how regional powers can take advantage of these vulnerabilities. Even when weak governments are not direct participants in bilateral disputes, the research shows that cyber wars can destabilize them by fostering new kinds of strategic rivalry.

CC BY

The research's ramifications go beyond Afghanistan to other vulnerable nations dealing with comparable difficulties brought on by regional cyberwarfare. The stability of digital infrastructure around the world is at risk due to the normalization of cyber spillovers as acceptable collateral damage, especially in areas with inadequate governance and weak cyber defensive capabilities.

Afghanistan's cyber vulnerabilities, according to realists, are a reflection of "larger trends in international relations in the digital age," where the anarchic structure of the international system makes it possible for more powerful nations to strategically take advantage of the digital infrastructure of their less powerful neighbors (Hamza, 2025). According to the report, cyberwarfare has become a crucial aspect of great power competition, posing new risks to governments that are sandwiched between superpowers.

While acknowledging the structural limitations that restrict policy alternatives, the suggested remedies, which are grounded in realist principles of strategic necessity and mutual benefit, provide workable methods for reducing cyber spillovers. The realist notion that cooperation can serve state interests when properly structured is shown in the emphasis on technological collaboration, the establishment of neutral infrastructure, and steps to foster confidence.

By offering insights that are pertinent to cybersecurity experts, governments, and international organizations tasked with safeguarding critical digital infrastructure, the research advances our understanding of the dynamics of cyber conflict in contested areas. The results of the study show how urgently new strategies for international cyber governance are needed in order to shield weaker states from the knock-on effects of big power cyberwarfare.

Future studies should look at the long-term effects of cyber spillovers on regional stability, the efficacy of suggested mitigation techniques, and the creation of global standards for the defense of neutral digital infrastructure. Weak governments like Afghanistan will continue to face difficulties due to the developing nature of cyber conflict dynamics and the introduction of new technology, necessitating continual research and creative policy solutions.

According to the study's findings, Afghanistan's experience should serve as a cautionary tale about the dangers of normalizing cyber spillovers as legitimate

CC BY

collateral damage in bilateral disputes. Neutral digital infrastructure preservation necessitates new forms of international cooperation that prioritize technical cooperation and mutual benefit over political agreements and can operate even in the absence of formal diplomatic connections. According to Hamza (2025), comprehending these processes is "important for developing effective policies that enhance security while maintaining strategic autonomy in a world that is becoming more interconnected but anarchic."

CC BY

References

Afghanistan Digital Security Report. (2023). Taliban-era cybersecurity challenges and regional implications. Regional Cybersecurity Institute.

Afghanistan Telecommunications Regulatory Authority. (2023). Annual telecommunications sector report 2023. Government of Afghanistan.

Ahmad, S. (2021). Pakistan's strategic dilemma in China-India rivalry. Institute of Strategic Studies Islamabad.

Bjelica, J., & Rutting, T. (2023). Digital Afghanistan: Telecommunications and internet under Taliban rule. Afghanistan Analysts Network.

Carnegie India. (2024). South Asian cybersecurity: Regional threats and responses. Carnegie Endowment for International Peace.

Creswell, J. W. (2018). Research design: Qualitative, quantitative, and mixed methods approach (5th ed.). Sage Publications.

Cyber Intelligence Report. (2021). Afghanistan cyber threat landscape post-Taliban. Regional Security Monitor.

Digital Frontier Foundation. (2021). Afghanistan internet disruptions: Regional cyber conflict impact. Digital Rights Assessment.

Economic Impact Assessment. (2024). Cross-border data flow disruptions in South Asia. Regional Economic Research Institute.

Financial Cyber Security Alert. (2025). Afghan banking sector under cyber threat. Financial Security Monitor.

Foschini, F. (2024). Taliban digital governance: Ideology meets technology. International Crisis Group.

Ameer Hamza. (2025). Caught in the crossfire: Pakistan cyber security dilemma in the India-China cyberwar (post Galwan Valley clash). Wah Academia Journal of Social Sciences, 4(1), 1101-1119.

Humanitarian Digital Infrastructure Report. (2024). Cyber impacts on humanitarian operations in Afghanistan. UN Office for the Coordination of Humanitarian Affairs.

International Trade Digital Infrastructure Report. (2024). Digital trade disruptions in conflict-affected regions. World Trade Organization.

Johnson, M., & Ahmad, R. (2022). Afghanistan's digital divide: Post-Taliban challenges and opportunities. Journal of South Asian Studies, 45(3), 234-251.

Morgenthau, H. J. (1948). Politics among nations: The struggle for power and peace. Alfred A. Knopf.

Regional Security Monitor. (2022). Operation Silk Route: Pakistani cyber operations in Afghanistan. Security Intelligence Analysis.

Rid, T. (2013). Cyber war will not take place. Oxford University Press.

Sanger, D. E. (2018). The perfect weapon: War, sabotage, and fear in the cyber age. Crown Publishers.

Sharma, A., & Gupta, S. (2023). India-Pakistan cyber warfare: Evolution and regional implications. Strategic Analysis, 47(2), 123-140.

Social Services Digital Impact Assessment. (2024). Cyber disruptions to healthcare and education in Afghanistan. Social Development Research Institute.

South Asian Cyber Watch. (2022). Operation Digital Crossroads: Indian cyber operations in Afghanistan. Cyber Intelligence Report.

CC BY

Taliban Digital Policy Analysis. (2024). Digital governance under Taliban rule: Contradictions and challenges. Afghanistan Policy Institute.

Threat Intelligence Report. (2025). Latest developments in Afghanistan cyber landscape. Regional Cybersecurity Analysis.

UN Digital Humanitarian Response. (2024). Cyber challenges in humanitarian operations: Afghanistan case study. United Nations.

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.

Waltz, K. N. (1979). Theory of international politics. Addison-Wesley Publishing Company.

World Bank. (2022). Digital Afghanistan: Connectivity and development challenges. World Bank Group.

CC BY