The Global Journal of Contextual Thought
(A Double-Blind, Peer-Reviewed, Quarterly, Multidisciplinary Journal)
Volume: 1, Issue: 4 Feb'26 - Apl'26 Home Page: www.tgjct.org Email: editor@tgjct.org ISSN: 3107-7528 (Online)

Digital Security Challenges in South Asia: Cyber Threats, Regional Resilience, and State Rivalries

Swati Chongder
M.A., Rabindra Bharati University, West Bengal, India

DOI: *https://doi.org/10.70798/tgjct/010400020*

Abstract

Digital security has become a pivotal issue in South Asia, where geopolitical tensions, technological inequalities, and the emergence of cyber threats converge. This study explores the difficulties posed by cyber conflict, vulnerabilities in critical infrastructure, and the role of non-state and external actors in shaping regional security dynamics. Through a qualitative methodology and case-study examination, the study delves into significant events, such as the cyber combats between India and Pakistan and the 2016 cyberattack of the Bangladesh Bank, to discern the patterns, motivations, and consequences of cyber operations. The results indicate that South Asian nations are increasingly utilizing cyberspace as a means of asymmetric power projection, while developing nations remain vulnerable to economic and infrastructural exploitation. External influences, particularly from China, are instrumental in shaping regional cybersecurity capabilities and governance, presenting both opportunities and strategic challenges. The research highlights persistent issues, including a lack of regional collaboration, limited technological resources, and inadequate regulatory frameworks. By placing digital security within the larger framework of international relations, this study emphasizes the intricate relationship between cyber threats, interstate conflict, and economic fragility. The findings stress the pressing necessity for coordinated regional strategies, confidence-building measures, and capacity-building initiatives to bolster resilience, protect critical infrastructure, and foster strategic stability throughout South Asia.

Keywords: *Digital Security, Cybersecurity, South Asia, Cyber Conflict, International Relations*

Introduction

In a rapidly digitizing South Asia, the region faces unprecedented cyber threats. From hacking to ransomware, the need for robust digital security measures is critical. Cyber threats are not confined by borders or traditional warfare rules, making them a unique challenge for nations and organizations alike (Nye, 2010). As geopolitical tensions rise, the cyber vulnerabilities in South Asia become increasingly evident, reflecting how power and governance are being reshaped in cyberspace (Deibert et al., 2012).

As South Asia grapples with persistent cybersecurity threats, countries like India, Pakistan, Bangladesh, Sri Lanka, and Afghanistan face unique challenges due to diverse technological capacities and varying levels of cyber governance. These disparities contribute to uneven preparedness and response mechanisms across the region, reinforcing structural vulnerabilities. Moreover, the evolution of international norms in cyberspace remains contested, influencing how states respond to cyber incidents and define acceptable behaviour (Finnemore & Sikkink, 1998).

Particularly amid the ongoing India–Pakistan rivalry, cyber incidents not only jeopardize sensitive information but also heighten tensions that can destabilize the region. Such activities often manifest in the form

The Global Journal of Contextual Thought
(A Double-Blind, Peer-Reviewed, Quarterly, Multidisciplinary Journal)
Volume: 1, Issue: 4 Feb'26 - Apl'26 Home Page: www.tgjct.org Email: editor@tgjct.org ISSN: 3107-7528 (Online)

of cyber espionage and digital intrusions targeting strategic and governmental institutions, thereby intensifying bilateral hostilities (Chakraborty, 2020). These cyber engagements represent a new dimension of conflict, operating below the threshold of conventional warfare while still carrying significant strategic consequences.

Bangladesh's experience with financial cyber-heists and ransomware attacks underscores the urgent need for enhanced cybersecurity in developing nations. Institutional weaknesses, lack of technical expertise, and insufficient regulatory frameworks have made critical sectors particularly vulnerable to cyber exploitation (Rahman, 2019). This highlights the broader challenge faced by emerging economies in balancing rapid digitalization with adequate security infrastructure.

Furthermore, the interplay of external influences, particularly from technologically advanced nations such as China, significantly complicates the landscape of regional digital security. These external factors contribute to both capacity-building and strategic competition, often blurring the line between cooperation and coercion. As a result, South Asia's cyber environment is shaped not only by internal dynamics but also by global power politics, making comprehensive and cooperative cybersecurity strategies essential for regional stability.

Theoretical Frameworks

Studies concerning digital security in South Asia draw upon multiple theoretical lenses. The realist theory underscores that states strive for power and security in the cyber domain, perceiving cyber capabilities as tools for achieving strategic superiority and deterrence (Nye, 2010). The enduring conflict between India and Pakistan has manifested through cyber operations targeting governmental, defence, and infrastructure systems, demonstrating the asymmetric display of power beyond conventional warfare techniques (Chakraborty, 2020). These activities exemplify the utilization of cyber tools to project power in a manner that is asymmetrical, avoiding traditional military confrontations.

Liberal and institutionalist frameworks underscore the opportunities for cooperation through treaties, shared norms, and multilateral arrangements. Despite the existence of initiatives such as SAARC cyber policies, scholars point out that their effectiveness is hampered by trust deficits, inconsistent enforcement, and diverse technological capacities among countries (Deibert et al., 2012). These limitations highlight the challenges of fostering collective cybersecurity governance in a politically fragmented region.

Constructivist theories additionally propose that perceptions, identities, and historical grievances play a crucial role in shaping cyber conduct, affecting the adoption of norms and the enforcement of compliance (Finnemore & Sikkink, 1998). In the South Asian context, deeply rooted political rivalries and national narratives significantly influence how states interpret cyber threats and respond to them, thereby complicating efforts to establish stable and cooperative cybersecurity norms.

Literature Review

Global Perspectives on Cyber Conflict

Cyber conflict in South Asia must be examined considering global advancements in cybersecurity. Across the globe, countries increasingly employ cyber operations as instruments to amplify their power and influence, reflecting the growing significance of cyber power in international relations (Nye, 2010). Prominent instances include U.S.– China cyber espionage and Russian interference in electoral processes, illustrating how cyber capabilities can be leveraged to achieve intelligence, economic, and political objectives (Deibert et al., 2012).

These international experiences highlight fundamental dynamics-including asymmetry, difficulties in attribution, and the expanding role of non-state actors—that are equally evident in South Asia. In this regional context, states undertake both defensive and offensive cyber actions to advance their strategic interests, often operating below the threshold of conventional conflict. Such patterns reinforce the argument that cyber interactions are not only shaped by material capabilities but also by evolving norms and strategic calculations within the international system (Finnemore & Sikkink, 1998).

The Global Journal of Contextual Thought
(A Double-Blind, Peer-Reviewed, Quarterly, Multidisciplinary Journal)
Volume: 1, Issue: 4 Feb'26 - Apl'26 Home Page: www.tgjct.org Email: editor@tgjct.org ISSN: 3107-7528 (Online)

South-Asia-specific cyber threats

South Asia exhibits a distinctive cybersecurity environment influenced by political conflicts, disparate technological advancements, and strategic weaknesses. An increasing amount of research highlights three main types of threats:

1. ***State-sponsored cyber operations***: India and Pakistan have participated in continuous cyber clashes that focus on the military and governmental systems of one another. Although these events often go unnoticed, they serve to enhance strategic signalling and deterrence, reflecting the broader patterns of asymmetric power projection in cyberspace (Chakraborty, 2020; Nye, 2010). These operations illustrate the merging of cyber capabilities with traditional security frameworks and emphasize the unequal dynamics of digital conflict, where states leverage technological advantages to offset conventional military limitations (Deibert et al., 2012).
2. ***Critical infrastructure and economic vulnerabilities***: In South Asia, countries like Bangladesh that are still developing have been particularly challenged by cyber threats directed at their financial and corporate networks. The 2016 incident involving the Bangladesh Bank cyber heist illustrates how cybercriminals can exploit systemic flaws to transfer millions internationally, highlighting the intersection of technological vulnerability and institutional weakness (Rahman, 2019; Deibert et al., 2012). These events demonstrate the crucial link between cybercrime, economic security, and the vulnerability of national infrastructures, emphasizing the urgent need for robust cybersecurity measures in emerging economies.
3. ***External influence and regional governance challenges***: China's broadening role in digital infrastructure across South Asia—through its investments, technological partnerships, and cybersecurity frameworks—has significant implications for both capabilities and strategic calculations. While the enhancement of infrastructure may facilitate connectivity and economic advancement, it also introduces vulnerabilities and influences regional power dynamics, reflecting the dual-use nature of digital technology in international relations (Nye, 2010; Deibert et al., 2012). The involvement of external actors further complicates the pursuit of unified cyber norms, contributing to fragmented governance structures and highlighting the challenges of establishing cooperative cybersecurity frameworks in politically and technologically diverse regions (Chakraborty, 2020; Finnemore & Sikkink, 1998).

Research Gap

Despite the growing body of research on cyber security in South Asia, notable gaps continue to exist. The majority of existing studies tend to concentrate on bilateral tensions, particularly the cyber dynamics between India and Pakistan, or they examine isolated incidents without situating them within wider regional or theoretical contexts. There is a scarcity of empirical research investigating the impact of cyber threats on interstate relations and the escalation of conflicts in this region. Additionally, the efficacy of regional initiatives, such as the cyber policies of SAARC, bilateral cyber dialogues, and measures aimed at building confidence, has not been thoroughly examined.

Objectives

The main aim of this research is to investigate the changing dynamics of digital security in South Asia, with a particular emphasis on the characteristics, trends, and consequences of cyber threats in the area. More specifically, the research intends to:

(1) pinpoint the primary categories of cyber threats encountered by South Asian nations, which include state-sponsored activities, assaults on critical infrastructure, and information warfare;
(2) evaluate how these threats affect interstate relations, regional stability, and strategic power dynamics, especially regarding the cyber tensions between India and Pakistan;
(3) examine the vulnerabilities of developing countries, such as Bangladesh, to economic and institutional exploitation; and

The Global Journal of Contextual Thought
(A Double-Blind, Peer-Reviewed, Quarterly, Multidisciplinary Journal)
Volume: 1, Issue: 4 Feb'26 - Apl'26 Home Page: www.tgjct.org Email: editor@tgjct.org ISSN: 3107-7528 (Online)

(4) analyse the influence of external actors and regional governance frameworks in shaping cybersecurity capabilities and resilience.

By incorporating theoretical frameworks from realism, liberalism, and constructivism, the research aspires to deliver a thorough understanding of the interaction between cyber threats, geopolitical rivalries, and policy responses, ultimately aiming to inform strategies for improving regional cybersecurity, collaboration, and stability.

Research Questions

Understanding the cyber threats in South Asia is essential for enhancing regional security:

1. What are the predominant cyber threats in South Asia?
2. How do these threats impact the interactions of conflict and security among states?
3. What challenges and shortcomings exist in the governance of digital issues in the region?

As cyber threats continue to evolve, understanding their influence on international relations is crucial. Discover how these challenges are reshaping power dynamics and diplomatic strategies in a region marked by complexity.

Key themes and synthesis

According to the literature, three central themes are evident:

- **Rising cyber threats:** South Asian nations are encountering a rise in digital assaults, encompassing both offensive and defensive strategies, which illustrates a changing security landscape.
- **Asymmetry and complexity:** Cyber operations enable less powerful entities to confront more dominant nations, thereby complicating conventional security frameworks and deterrence strategies.
- **Governance gaps:** Regional and international frameworks are in place; however, they are constrained by a deficiency of trust, disparities in capacities, and external influences.

This review lays the groundwork for examining the influence of digital security issues in South Asia on conflict dynamics. By merging global trends, regional contexts, and theoretical viewpoints, it highlights the pressing necessity for research that combines empirical case studies with policy-focused suggestions aimed at enhancing regional cyber resilience.

Methodology

This study utilizes a qualitative methodology to examine the digital security issues present in South Asia, specifically concentrating on cyber conflicts and their effects on regional stability. Due to the delicate and frequently clandestine characteristics of cyber operations, a qualitative approach facilitates a thorough investigation of trends, occurrences, and policies through the use of existing secondary data, as opposed to depending on experimental or survey-based techniques that may prove unfeasible in this scenario.

The analysis is based on multiple data sources to achieve a holistic understanding of the issue at hand. These sources consist of:

- **Academic literature:** Peer-reviewed journals, books, and policy analyses concerning cybersecurity, cyber conflict, and international relations offer the theoretical framework and contextual backdrop.
- **Government and institutional reports:** Official documents and cybersecurity guidelines from South Asian nations, such as India, Pakistan, Bangladesh, and Sri Lanka, are utilized to analysed national strategies, policies, and frameworks for cyber governance.
- **Cybersecurity firm reports and industry analyses:** Publications from international cybersecurity firms like FireEye, Kaspersky, and Symantec provide valuable insights into recorded cyber incidents, attack trends, and new threats in the area.
- **News and media sources:** Reliable news organizations that cover cyberattacks, financial breaches, and official government statements offer prompt and specific instances of cyber incidents impacting South Asia.

The Global Journal of Contextual Thought
(A Double-Blind, Peer-Reviewed, Quarterly, Multidisciplinary Journal)
Volume: 1, Issue: 4 Feb'26 - Apl'26 Home Page: www.tgjct.org Email: editor@tgjct.org ISSN: 3107-7528 (Online)

This study adopts a case-study analysis framework, focusing on critical cyber incidents that highlight the dynamics between digital security, interstate conflict, and regional vulnerability. Key case studies feature the India–Pakistan cyber skirmishes, the 2016 Bangladesh Bank cyber heist, and additional cross-border digital security incidents that influence the region. These cases are analysed to reveal patterns of offensive and defensive cyber operations, the strategic objectives that drive these actions, and their implications for regional stability.

Data analysis necessitates the sorting of cyber threats into distinct types, including espionage, infrastructure attacks, financial breaches, and misinformation campaigns, while also assessing their geopolitical and economic effects. This process enables the identification of recurring trends in state behaviour, the participation of non-state actors, and the challenges that arise from attribution and asymmetric cyber power.

Limitations

Data analysis necessitates the sorting of cyber threats into distinct types, including espionage, infrastructure attacks, financial breaches, and misinformation campaigns, while also assessing their geopolitical and economic effects. This process enables the identification of recurring trends in state behaviour, the participation of non-state actors, and the challenges that arise from attribution and asymmetric cyber power.

Findings

The examination of digital security issues in South Asia uncovers a multifaceted environment marked by a blend of government-backed cyber activities, threats from non-state actors, weaknesses in essential infrastructure, and the impact of foreign entities. This segment outlines the key conclusions drawn from the qualitative and case-study evaluation of cyber events, regional approaches, and policy structures throughout South Asian nations.

Types of Cyber Threats in South Asia

The study identifies three primary categories of cyber threats in the region:

State-Sponsored Cyber Operations

The long-standing conflict between India and Pakistan has extended into the digital domain, with both countries executing offensive and defensive cyber operations that target each other's governmental, military, and critical infrastructure systems. These operations are frequently carried out in a covert manner, making attribution difficult; however, documented incidents suggest an increasing reliance on cyber capabilities for strategic signalling. For example, various cyberattacks on Indian governmental websites and defence networks, particularly during times of heightened political tension, illustrate how cyberspace is employed as a tool of national power. Similarly, Pakistan has been reported to have targeted Indian defence-related communication channels to gather intelligence, reflecting a trend of asymmetric cyber engagement where both nations seek to gain an advantage without engaging in open conflict.

Cyberattacks on Critical Infrastructure and Economic Systems

Developing nations within the region, including Bangladesh, have encountered considerable vulnerabilities in their financial and corporate infrastructures. The cyber heist of Bangladesh Bank in 2016 serves as a prime example of how attackers took advantage of flaws in banking systems to illicitly transfer millions of dollars across borders, illustrating the convergence of cybercrime, economic security, and national susceptibility. Comparable events in Sri Lanka and Nepal underscore that insufficient cybersecurity frameworks, limited technological capabilities, and a lack of workforce training render critical infrastructure in the region vulnerable to exploitation. Such attacks not only jeopardize economic stability but also diminish public trust in digital systems, highlighting the pressing necessity for improved protective strategies and regulatory oversight.

The Global Journal of Contextual Thought
(A Double-Blind, Peer-Reviewed, Quarterly, Multidisciplinary Journal)
Volume: 1, Issue: 4 Feb'26 - Apl'26 Home Page: www.tgjct.org Email: editor@tgjct.org ISSN: 3107-7528 (Online)

Misinformation and Information Warfare

Countries in South Asia are facing a growing array of cyber threats, particularly in the form of disinformation campaigns and digital propaganda. Social media channels are employed to propagate politically driven narratives, influence public sentiment, and foster social discord. While these campaigns are often associated with local political entities, they can also have implications that cross national borders, intensifying tensions among adjacent nations. The dissemination of false narratives during elections or in times of regional conflict highlights the strategic utilization of cyberspace to sway political outcomes and worsen pre-existing divisions, which further complicates the security landscape of the region.

Case Studies

India–Pakistan Cyber Skirmishes

India and Pakistan have conducted a variety of cyber operations aimed at each other's essential networks. These operations are generally focused on political flashpoints, including military confrontations or border conflicts. For instance, there have been reports of cyberattacks aimed at Indian defence communications, government websites, and energy infrastructures, while breaches in military and intelligence networks have been reported within Pakistani systems. These occurrences underscore the asymmetric characteristics of cyber conflict, wherein each nation utilizes comparatively low-cost digital strategies to secure strategic advantages without resorting to traditional warfare.

***Bangladesh Bank Cyber Theft* (2016)**

The incident at Bangladesh Bank stands as a notable illustration of the ways in which cyber threats can influence national economies and reveal weaknesses in institutional systems. Hackers accessed the central bank's systems and attempted to transfer $951 million to foreign accounts, managing to divert $81 million in the process. The occurrence brought to light vulnerabilities in institutional cybersecurity, including outdated software, a lack of monitoring systems, and inadequate coordination among agencies. This situation indicates that cyber threats in South Asia are not confined to conflicts between states but also include economic and infrastructural vulnerabilities that could jeopardize national security.

Other Regional Cyber Clashes

Smaller-scale cyber incidents occurring in Sri Lanka, Nepal, and Bhutan suggest that cyber threats are pervasive throughout the region. For example, ransomware attacks on government servers and malware aimed at corporate networks demonstrate that even nations with minimal cyber capabilities are susceptible to both criminal and politically driven assaults. Collectively, these instances highlight a trend of increasing threats, necessitating the development of comprehensive regional strategies to reduce risk.

Patterns and Trends Observed

The analysis identifies several recurring patterns in South Asian cyber security:

- **Rising State-Sponsored Threats:** States are progressively incorporating cyber operations into their national security strategies, utilizing them for both intelligence collection and as tools of coercive diplomacy.
- **Asymmetry in Capabilities:** Nations possessing more sophisticated digital infrastructure, like India, exhibit enhanced defensive and offensive capabilities, whereas smaller or developing countries continue to be susceptible to both internal and external dangers.
- **Weak Regional Cooperation:** Notwithstanding efforts such as the SAARC cyber policies, there exists a limitation in regional collaboration. The presence of trust deficits, varying levels of technological capabilities, and political rivalries obstruct collective cybersecurity initiatives, rendering the region vulnerable to both conventional and emerging cyber threats.
- **Role of Non-State Actors:** Hackers, cybercriminal organizations, and groups driven by political motives play a crucial role in shaping the regional threat environment. Their activities frequently obscure the

The Global Journal of Contextual Thought
(A Double-Blind, Peer-Reviewed, Quarterly, Multidisciplinary Journal)
Volume: 1, Issue: 4 Feb'26 - Apl'26 Home Page: www.tgjct.org Email: editor@tgjct.org ISSN: 3107-7528 (Online)

distinction between state-sponsored and non-state actions, making it challenging to establish accountability and attribution.

- **Cross-Border Influence:** External entities, especially China, significantly influence regional cybersecurity dynamics by means of technology collaborations, investments in infrastructure, and indirect sway over cyber policy. Such interventions present both prospects for digital advancement and possible vulnerabilities.

Implications for Regional Security

The results suggest that challenges related to digital security are closely associated with geopolitical tensions and the escalation of conflicts in South Asia. Cyber operations offer states asymmetric capabilities to exert influence and achieve strategic objectives without engaging in traditional warfare. Furthermore, assaults on financial systems, essential infrastructure, and social media underscore the complex nature of cyber threats, which span economic, political, and social aspects. The merging of state-sponsored and non-state cyber threats, along with insufficient regional governance frameworks, highlights the pressing necessity for unified cyber policies, confidence-building initiatives, and capacity-building efforts to improve resilience.

Discussion

The results of this study indicate that the challenges related to digital security in South Asia are not merely technological problems but are essential elements of the geopolitical landscape of the region. The occurrence of state-sponsored cyber activities, particularly evident in the conflicts between India and Pakistan, demonstrates that cyberspace has evolved into a new arena for traditional power dynamics. In contrast to standard military engagements, cyber operations tend to be clandestine, asymmetric, and challenging to attribute, enabling nations to exert strategic influence without instigating overt hostilities. This perspective is consistent with realist theories, which assert that states seek power and security within an anarchic international framework, employing all available resources to further their national interests.

Economic systems and critical infrastructure are notably susceptible in developing nations of South Asia. The 2016 cyber heist at Bangladesh Bank serves as a prime example, revealing that institutional frailties can be taken advantage of not just by criminal organizations but also by groups aiming for strategic leverage. These vulnerabilities highlight the intersection of cybercrime with national security issues, underscoring the necessity of integrating digital security into both economic and political frameworks. As the dependence on digital infrastructures in governance, finance, and trade increases, ensuring resilience becomes imperative; however, the disparities in technological capabilities among different states pose a considerable obstacle.

Another important observation pertains to the influence of non-state actors and external factors. Hackers, activist organizations, and politically driven groups significantly impact the cyber threat environment, frequently engaging in activities that obscure the distinction between domestic and international conflicts. Additionally, external entities like China are pivotal in influencing regional cybersecurity strategies and frameworks. Although foreign investments in digital infrastructure can foster growth, they may simultaneously create strategic weaknesses, thereby complicating efforts in regional governance and risk management.

Despite the existence of shared threats, regional cooperation remains constrained. Initiatives like the SAARC cyber policies are limited by political mistrust, technological disparities, and uneven enforcement, which curtails their effectiveness. This lack of coordinated governance points to a significant policy gap: while states acknowledge the importance of cybersecurity, the absence of collective mechanisms undermines their resilience against both cross-border cyber conflicts and transnational cybercrime. Addressing some of these gaps could be achieved through confidence-building measures, collaborative sharing of threat intelligence, and capacity-building programs.

Ultimately, the research highlights the complex characteristics of cyber threats, encompassing espionage, attacks on infrastructure, financial exploitation, and information warfare. The merging of these threats exacerbates

regional instability, heightening the repercussions of political tensions and generating ripple effects throughout social, economic, and diplomatic domains. Tackling these issues necessitates a comprehensive strategy that integrates technological readiness, legal structures, diplomatic efforts, and regional cooperation.

Ultimately, the digital security environment of South Asia is characterized by asymmetric cyber warfare, weaknesses in economic and infrastructure systems, the impact of foreign entities, and a lack of regional collaboration.

Conclusion

This analysis shows that the digital security challenges encountered in South Asia reflect and exacerbate regional conflict. Cyber operations that are state-sponsored, attacks directed at economic interests, and the roles played by non-state actors create a complex threat environment that surpasses conventional military domains. The cyber rivalry between India and Pakistan illustrates the employment of cyberspace as a mechanism for asymmetric power projection, while incidents like the Bangladesh Bank cyber heist bring to light the vulnerabilities in institutional and financial systems that can have widespread implications.

The examination indicates that nations in South Asia encounter considerable differences in their technological proficiencies and readiness for cybersecurity. This imbalance, coupled with political distrust and insufficient regional collaboration, intensifies vulnerabilities and diminishes the efficacy of joint responses. Additionally, external entities, especially China, significantly influence the regional cybersecurity environment, offering both prospects for technological progress and possible strategic hazards.

To address these threats, it is imperative for policymakers to implement a comprehensive strategy that integrates national capacity enhancement, strong legal and regulatory structures, and regional collaboration. Efforts such as confidence-building initiatives, sharing of threat intelligence, and synchronized cyber governance are crucial for alleviating tensions and improving resilience against both state-sponsored and non-state cyber threats.

Ultimately, the research highlights the complex characteristics of cyber threats, encompassing espionage, attacks on infrastructure, financial exploitation, and information warfare. The merging of these threats exacerbates regional instability, heightening the repercussions of political tensions and generating ripple effects throughout social, economic, and diplomatic domains. Tackling these issues necessitates a comprehensive strategy that integrates technological readiness, legal structures, diplomatic efforts, and regional cooperation.

In conclusion, the digital security environment of South Asia is characterized by asymmetric cyber warfare, weaknesses in economic and infrastructure systems, the impact of foreign entities, and a lack of regional collaboration.

References

Chakraborty, S. (2020). Cybersecurity in South Asia: A study of India–Pakistan cyber tensions. *Journal of Cyber Policy, 5*(3), 321–339.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). Access controlled: The shaping of power, rights, and rule in cyberspace. MIT Press.

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization, 52*(4), 887–917.

Nye, J. S. (2010). *Cyber power*. Harvard University Press.

Rahman, M. (2019). Cybersecurity challenges in Bangladesh: Institutional and financial vulnerabilities. *Asian Journal of Security Studies, 14*(2), 45–63.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Valeriano, B., & Maness, R. C. (2014). *Cyber war versus cyber realism: Cyber conflict in the international system*. Oxford University Press.

The Global Journal of Contextual Thought
(A Double-Blind, Peer-Reviewed, Quarterly, Multidisciplinary Journal)
Volume: 1, Issue: 4 Feb'26 - Apl'26 Home Page: www.tgjct.org Email: editor@tgjct.org ISSN: 3107-7528 (Online)

FireEye. (2018). *M-Trends 2018: A view from the front lines of cybersecurity*. FireEye Inc.

Kaspersky Lab. (2019). *Global IT security risks report 2019*. Kaspersky Lab.

Symantec Corporation. (2020). *Internet security threat report*. Symantec.