International Journal for Conventional and Non-Conventional Warfare

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

Framing the Digital Threat: Cybersecurity and Strategic Narratives in India-Pakistan Relations

Jannat Naseeb is pursuing her MS. Security and Strategic Studies from University of Management and Technology.

Abstract

The cyber confrontation between India and Pakistan has become major features for the strategic rivalry between both states. It is shifting their neutral use of digital advancements to critical cyber-espionages and attacks. This research is going to explore securitization of cyberspace by India and Pakistan under the lens of Securitization Theory, which tried to explain how both states framed cyberspace as a existential threat and it requires extraordinary measures. It examines the key cyber-attacks between 1999 and 2025 like hacking of websites, malware activities, espionage activities, as well as government and military network attacks. This study provides an overview of the core components of securitization process using qualitative content analysis of cybersecurity reports, academic research, government documents, and open-source intelligence to estimate the cases of referent objects of digital sovereignty and critical infrastructure, the presence of securitizing actors (national security agencies and political leadership), and a process of framing cyber threats as existential in character. The study describes the incidents in which both nations have cited cyber incidents as a justification of widened surveillance, the development of offensive capabilities in cyberspace, and cyber militarization. The significance of this research is that it couples cyber conflict and the concepts of strategic regional instability and that the digital world should adhere to some rules of conduct. The study also helps to understand cyber deterrence, dynamics of escalation and lack of formalization in the interstate interactions in the cyber sphere in South Asia by tracing the strategic rationality of the specified cyber operations. It comes to the conclusion of the research that unless both states show common interest in some bilateral cyber confidence-building measures and become a participant of global cyber norms, cyberspace will be an unsafe unregulated battlefield in the already weak security system.

Keywords: Cyberspace, Warfare, Existential Threat, Security, Securitization Theory, Framing

Introduction

Cyber warfare in cyber space has made the cyber security a matter of importance to the state. This research paper on this new era of national cyber security methods reveals the most important breakthroughs in policy making process of government but because of the convenience of the subject, cyber security is taken to the level of government priorities. On the basis of these strategies, it has been generally assessed that the government, the network and Information and Communication Technologies (ICTs) are fundamental to monetary and social development. The free Internet and ICTs are one more resource of growth and an engine of growth, social wellbeing and personal expression in the scenario of monetary

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

decline on the whole. The Internet economy is growing along with governments, so as the economy and society as a whole continue becoming increasingly reliant upon this computerized system to act out its core functionalities.

Not only India and Pakistan are both nuclear states but also both have traditional military strategies along with both having engaged in virtual war of words and attempts to destroy each other through hacking the safe and confidential information since 1990s (Fazzini, 2019). The international relations are getting diluted as they are highly mobilized. The society now learns through studying the facilities of message and communication (Alker, 2011). Both the states are effectively availing cyber warfare in achieving the regional goals in the south Asian region, particularly to stay hegemonic and to extend influence in the south Asia. India is always in the breach of the line of control but the international law is also violated in case of international law the targeting civilians or moving close to the border cannot be put place during the time of peace. India on the other hand, never tries to do justice to image of Pakistan as she always tries to mislead and maneuver the world media. A group based in Karachi University supported by the RAW was trapped at the end of March 2020, supplying terror and propagation efforts that turn against Pakistan (Khan, 2020).

This kind of activity is escalating the threat of war which raises serious security indicators in Pakistan. The cyber warfare applications employ various skills and various methods. As a day, Cyber warfare is a significant menace in the South Asian region which in the past used to affect the opponent. New technologies are rapidly appearing and entering into the strategy of both states, Pakistan and India. This study will have the aim of checking the effect caused by cyber war of Pakistan and India in the region. Cyberspace as a valuable instrument has created an arena through which nationalistic and fanatical hackers get to voice out their patriotism and belittle the opponent on both ends. Cyberspace is operating as Advanced Persistent Threats (APTs) as well, but these patriotic and activist groups have an excellent grip and connection with the institutions of state, they are operating to spy and will steal information in order to reach the strategic targets. APTs employ various methods such as speech phishing when accessing contact and over in to the enemy network then infect them with various viruses such as malware of spying (Khalil, 2020). This paper scrutinizes cyber war between Pakistan and India.

India Pakistan cyber operations go further than classic hacking methods and are complex in nature and comprise advanced intelligence collection, infrastructure destruction, and psychological war operations. Advanced illegal programs, focused attacks, and proper digital actions have grown to be the most important sources of their continued situation battle. These operations obscure the boundaries between the customary military action and warfare waged by technologies. Cyberspace has become an important sphere of psychological operations and both countries take advantage of the digital platforms to alter the view of the people, propagate false information, and destroy the reputation of the institutions (Rahman et al., 2021).

The India-Pakistan digital war is a wider shift in the nature of conflicts in the world, where technological advantages become key determinants of the strength of a nation (Khan et al., 2019). Their online wars provide a clue to how new technologies are changing the nature of geopolitical relations that question the conventional concept of sovereignty over land and strategic interest. The India-Pakistan cyber rivalry will probably get more compounded and profound as machine learning, Thursday artificially intelligent, and quantum computing

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

become utilized. The next-generation cyber operations could be marked by the likely adoption of autonomous systems, enhanced algorithm-based tactics of warfare, and unmatched technological sophistication (Hussain et al., 2021).

Literature Review

The increase in the cyber warfare between India and Pakistan can be witnessed by focusing on modernization of the conventional form of warfare to the asymmetric pattern of war and normalize the war over the nuclear ability (Since the 1990s, both India and Pakistan have been waging the cyberspace to fight espionage, website defacing, distributed denial of service (DDoS) and phishing but these endeavors can be viewed as a modern version of the fifth-generation warfare (Ahmad and Jahangir, 2025; Pakistan Review, 202 Several instances have been reported where Indian Advanced Persistent Threats (APTs) and the hacktivist organizations in Pakistan that go by names True Cyber Army and Indian Cyber Army have attacked one another in their crtical infrastruktur (ResearchGate, 2020; Wikipedia, 2025).

The rise of this warfare is greatly emphasized upon in the years 1999-2001 where by there was a drastic rise in the number of annual attack in comparison to the preceding year which was 275 assaults annual as opposed to 45 more attacks the previous year. As is the case with Pakistan, such intense cyberspace operations are sounding alarm bells as they have the capabilities of causing serious harm to military, government, and currency systems due to destabilization and theft of secrets-intelligence (Pakistan Review, 2022; Mustafa et al., 2020). The cyber front has now become a prestigious ground of battle because of the low-cost of attribution and asymmetrical advantage it inflicts (Mustafa et al., 2020). The fact that this change of strategy not only welcomes the restrictions of the nuclear age but also shares the cry of national cybersecurity resilience.

The build up of the cyber capability in the country was in a gradual process through institutional lever such as National Cyber Security Policy (2013) and organization such as specialized units under NTRO (National Technical Research Organisation).

It is strongly emphasized that the escalation of this conflict did not lessen in the 1999-2001 period when the incidents of cyber attacks in a single year rose at a high margin of 275 attacks in 1999-2001 as compared to 45 in the preceding year. In the example of Pakistan, it is making alarm bells due to severe damage that can be caused in the military, government, and monetary systems due to destabilization and theft of secrets-intelligence (Pakistan Review, 2022; Mustafa et al., 2020). The cyber front has become a great battle ground because the risk of attributed is small, and the advantage is asymmetrical (Mustafa et al., 2020). In addition to throwing oneself into the constraints of the nuclear age, this shift of direction delivers those national cries to cybersecurity resilience. The nation established cyber capability over a period of constancy using institution mechanism such as National Cyber Security Policy (2013), organization such as specialist bodied under NTRO (National Technical Research Organisation) (Imran & G. Murtiza, 2022; Pakistan Review, 2022).

Scholarly discussions indicate that the cyber security system in Pakistan is still primordial, which is further aggravated by the ineffective legislation and the lack of policy enforcement (Ahmad & Khan, 2022; JPSP, 2023). At the same time, though the Prevention of Electronic Crimes Act (2016) provides the legal framework upon which strict laws should be based, the implementation of law is still inconsistent (Dimension of Cyber Warfare, 2023). The presence of national organizations like NCCS (created in 2018), PKCERT (in 2024), and NCCIA (in 2024) signify a continued attempt to beef up Pakistani cyber resiliency, but the detection,

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

response, and training of the workforce remain weak, according to research studies (Ahmad & Khan, 2022; JPSP, 2023). Insufficient cyber preparedness, Pakistani researchers warn, may enable the hostile to take advantage of digital infrastructure systems such as banks, e governance programs, and databases operated by NADRA (Ahmad & Khan, 2022). Moreover, the internal vulnerabilities and the mistrust of the population are worsened by cybercrime and terrorism, including hacktivism (Ahmad & Khan, 2022; JDSS, 2022). Importantly, the literature highlights the necessity to use the comprehensive integration of policies including legislative transformation and the strengthening of institutional capabilities, and the cooperation of the public and entrepreneur sectors in order to reduce the risks of cyber-threats and defend the national interests (JPSP, 2023; Dimension of Cyber Warfare, 2023).

The cyber duplication enhances India Pakistan tensions that have been in existence; the scholars assert that the unpredictability of escalation chains increases the risk of miscalculation that escalates into the sphere of physical conflict (Ahmad & Jahangir, 2025). Since both nations have nuclear weapons, the cost of a misunderstanding caused by a cyberattack or the collateral technical destruction caused by the same is truly astronomical (Ahmad & Jahangir, 2025; Ashraf & Kayani, 2023). Attribution is still complicated by the intricate nature of non-state actors and cyber proxies, which restrains the use of strategic deterrence capabilities (Mustafa et al., 2020). New tools proposed recently to manage cyber conflicts include cyber-confidence-building measures (CBMs) and the mutual deterrence procedures in an attempt to increase understanding of and to coordinate response to incidents However, political suspicion and secrecy work against compliance. Pakistani writers reveal that a bilateral hotline in the cyberspace, information exchange system, and the third party intervention are needed to deescalate cyber emergency. Devoid of such actions, the cyber conflict can reduce the regional peace construction as well as generate more instability and exacerbate competition in the emerging fields of technology.

In the literature, the problem of cyber threats is conceptualized as a central pillar in the paradigm of national security in Pakistan and not as some digital pests (Imran & G. Murtiza, 2022; Ahmad & Khan, 2022). Economic stability and citizens confidence may be under threat with successful attacks to critical infrastructure and also is the risk of espionage. At the same time, there is domestic cyber-criminality and terrorism to take into consideration. In their study, Pakistani researchers do propose a multifaceted approach to national practice: through the enhancement of institutional preparedness through both NCCIA and PKCERT, improvement of cyber law, focus on capacity-building, and industry-academia collaboration. Engagement with the region on the lines of cyber diplomacy, confidence-building measures and even working along with international partners may help protect Pakistan against the wider threats on the digital landscape. In addition, new cyber-technologies, including turnkey offensive kits, pose some threat and opportunity (Bouke & Abdullah, 2023), which is why international participation in cyber norms and regulations should be considered active. Finally, bridging the cyber capability gap with India, decreasing the dependency on external cyber capabilities, and formalization of cyber resilience will be required in order of national sovereignty and strategic stability of and to Pakistan.

Securitization Theory

Securitization Theory, as formulated by the Copenhagen School most notably Ole Wæver—aids in the conceptualization of un-(tradition)al threats, like cyber warfare, as matters of

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

security. If a certain problem is presented by a securitizing actor as an existential threat to a referent object, then the needed act will be done per audience acceptance (Buzan et al., 1998). (Wæver, de Wilde, and Buzan, 1998). In the context of India as well as Pakistan, two nuclear-armed rivals with a history of conflict, the securitization within cyberspace has greatly strengthened since the late 2000s because cyber operations together with mutual espionage plus disinformation campaigns have risen. In securitization, the referent object is that which is threatened. This object has to also be protected now.

In the situation with India, the referent objects have gone beyond the traditional state sovereignty to the areas of power grids, defense networks, and financial systems publicized by the trust in electoral institutions. In the same manner, in the case of Pakistan, the referent objects have become more modified and enriched by adopting military networks, strategic databases such as NADRA and national cohesion especially when one considers instances of perceived cyber-espionage by India. These referent objects are not only representative of technological weaknesses, but of basic constituents of sovereignty and national integrity in operation.

In both countries, state institutions are the ones who proclaim a certain issue as a security threat and thus the securitizing actors. The National Technical Research Organization (NTRO), the ministry of Home Affairs, and the political leaders in India have time and again expressed concerns over Pakistani cyber activity, particularly after other events like the 2008 Mumbai attacks and the 2019 Pulwama-Balakot conflict. The Pakistani hacker groups are commonly discussed in the media in India as cyber-terrorist groups, which can also increase the sense of an existential threat (Chaudhuri, 2021). On the Pakistani side, there are several institutions that contribute to the representation of Indian cyber activities as the part of a larger campaign to undermine the internal Pakistan system and digital sovereignty, including Inter-Services Public Relations (ISPR), Pakistan Telecommunication Authority (PTA), and the Ministry of IT and Telecommunication (Aziz, 2020).

Existential threat to the cyber context between India and Pakistan has been tendentiously explored in terms of cyber attacks which have been either pinned on or directed at the other. India refers to the menace of Pakistani malware attacks on military personnel (e.g., the so-called spyware campaign company) and the chances of cyber sabotage of national strategic targets (Singh, 2020).

Pakistan has on the contrary accused Indian state sponsored actors of hacking sensitive databases, disruption to communication and media systems, including the 2023 NADRA breach. These threats are not packaged only as a technology and intelligence problem but as a crisis of existence which could jeopardize national survival, stability, as well as the state security architecture.

Such extraordinary actions taken by the two states indicate how deep securitization goes. India has already created its Defense Cyber Agency and is in the process of developing one National Cybersecurity Strategy that is intended to enhance offensive and defensive cyber capacity. Pakistan has enacted Prevention of Electronic Crimes Act (PECA), has expanded surveillance programs and has proposed a National CERT (Computer Emergency Response Team). The two states have also conducted retaliatory campaigns in cyberspace and strengthened cyber command systems in what is more than normal practicing of cybersecurity policies because such moves are a form of securitization response (Hussain & Arshad, 2022).

International Journal for Conventional and Non-Conventional Warfare

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

The example of securitization of the cyberspace between Pakistan and India demonstrates that digital space is no longer a marginal issue that is peripheral to national security thought. It justifies the application of extraordinary state authority, for example, of surveillance, censorship as well as cyber retaliation, frequently with little transparency or accountability. Although securitization can help prepareness, it can also cause tensions to increase, curb civil liberties and create a regional cyber-arms race. Such prompts the significance of critical review of the practice of securitization towards a qualitative development of responsible state actions and cyber stability of the area.

Cyber Confrontation Between India and Pakistan: A Timeline of Escalation and Strategic Messaging

The geopolitical tensions between India and Pakistan, which are very old, their recent development has opened another frontier to the geopolitical conflict cyberspace. An activity characterized initially by low-level digital skirmishes has turned into advanced cyber espionage, disinformation campaigns, and even direct attacks on the critical infrastructure. The nature of these confrontations is not tactical, but rather is quite strategic as it is more related to national security requirements and the competition of power dynamics. Based on the cyber realism and securitization theory, these incidences depict how the two countries have weaponized cyber space according to their security doctrine.

1. In 1999 Kargil War

The most significant cyber conflict so far tracked was that witnessed in the Kargil War in 1999 when a hacker group that was pro-Pakistan group known as GForce hacked into the websites of the Indian government to deliver political messages and cause havoc to the state communication. It was an example of symbolic and amateur attack in today-terms, but it was the first example of entering cyberspace into Indo-Pak hostilities and it was one of the first examples of a psychological attack on people, perception.

2. Mumbai attack of 2008

The Mumbai attacks of 2008 marked a start in India towards a shift in thinking about cybersecurity. It was also identified that the terrorists communicated by means of encrypted tools and Voice over Internet Protocol (VoIP) voice services to organize the attack. Also, this was not a direct cyberattack but a case of securitization in the context of the cyberspace that resulted in the investment in intelligence gathering and surveillance abilities (Chaudhuri, 2021). It also pointed to the introduction of digital tools to traditional terrorism.

3. 2013 Operation Hangover

In 2013, Norman cybersecurity company learned that a suspected Indian cyber-espionage operation, known as the Operation Hangover, employed malware to enter the Pakistani defenses and infiltrate its networks used by its diplomats. This operation demonstrated that the extent of covert cyber capabilities in intelligence gathering was deep-seated despite India denying its culpability and this undoubtedly in line with the line of thinking of cyber realism that perceives cyberspace as a fresh domain of state-sponsored espionage and strategic superiority.

1. Attack at the Pathankot airbase in 2016

The 2016 Pathankot airbase attack was an alleged case of allying Pakistani-based cyber-enterprisers who made a reconnaissance of the airbase terrain upon visiting the facility with phishing and data collection before physical attack. This shows the capability of the cyber operations to be employed alongside the kinetic battles such as hybrid warfare.

International Journal for Conventional and Non-Conventional Warfare

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

2. Cyber-espionage campaign 2017 and 2018

In 2017 to 2018, Pakistani APT group Stealth Mango (APT36) was claimed to have been involved in large-scale cyber-spying against Indian military officers and diplomats with Android-based spying malware. The spyware could retrieve sensitive documents, emails as well as deduce the Global Positions System data on the targeted devices. It was implied by these developments that Pakistan was also gaining offensive cyber capabilities, which it used to gain asymmetric intelligence (Hussain & Arshad, 2022).

1. **Pulwama attack and the Balakot air strikes 2019**

The fiercest episode of cyber warfare presented itself after the 2019 Pulwama attack and Balakot air strikes. Days and weeks after these happened, both nations experienced a surge in cyber activities. Pakistani websites were defaced by Indian hackers and Pakistani hackers are said to have conducted a DDoS (Distributed Denial of Service) attack as well as some disinformation on Indian social media sites. Such operations turned out to be not only retaliatory but also psychologically and narratively oriented, aimed at reshaping the belief of the masses in the context of one-sided geopolitical arrogance.

2**. COVID-19 Pandemic 2020**

Cyber conflict changed its shape during the COVID-19 pandemic in 2020. S Pakistani-based organizations were also blamed of attacking Indian medical facilities and vaccine-development labs. Meanwhile, it is claimed that India stepped up on monitoring of Pakistan cyber activity. It was the next stage of cyber warfare exploitation, crisis-to-disruption (Aziz, 2020).

1. Alarms of Digital Sovereignty 2023

In 2023, perhaps one of the most important was when Pakistani intelligence sources alleged that Indian APTs accessed NADRA, Pakistan national database authority, stealing biometric and identity information of millions. Although the Indian government did not admit any action, Pakistani agencies discussed this event as an example of Aggressive digital posturing by India. This event posed serious concerns about digital sovereignty and cyber deterrence and the policy change to create a National CERT in Islamabad.

2. 2025 Reciprocal Cyber Escalation

In 2025, two countries supposedly entered into a cyber escalation, after skirmishes were reported in the Line of Control. It was said that India had also attacked the military communication system and encryption data transmission system of Pakistan and Pakistan retaliated by attacking the power grid control points and state-run railway systems of India. Although both governments refused to take immediate acknowledgement of responsibility, security experts attributed odd system failures and synchronised digital mischief in both nations. It is estimated that this occurrence is the first one during which cyber attacks are considered officially, as a part of larger conflict strategy, but then again, officially unofficially, illustrating the fact that the cyberspace is a battlefield now.

Across these events, certain trends become clear: both India and Pakistan are moving from symbolic acts like website defacements to strategic cyber operations targeting military, political, and economic systems. Cyber warfare has evolved into a central tool for asymmetric deterrence, intelligence gathering, and information control. As these operations become increasingly sophisticated and state-sponsored, they also heighten the risk of escalation and miscalculation.

International Journal for Conventional and Non-Conventional Warfare

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

Ways To securitize cyberspace

Avoidance of cyber warfare between Pakistan and India and establishment of a more peaceful and secure cyberspace necessitate an entire spectrum of suggestions, including enhancement of cyber security, promotion of dialog and international collaboration. Some of the important recommendations are as follows:

Foster Diplomatic Activities and Confidence-Building Measures (CBMs): India and Pakistan need to start formal dialogue aimed at cyber security in order to stipulate the rules, minimize distrust, and avoid misunderstanding of cyber operations as the acts of war. Bilateral **Cybersecurity Dialogue:** Frequent visits of the cybersecurity representatives between the two nations can be brought under common consonance and then problems related to critical infrastructural conservation, military-oriented operations in Wars can be tarried. space, and potential use of the cyber as the tool of spying or aggression must be addressed

Confidence-Building Measures (CBMs): Create CBMs that is specific to cyber security in order to foster transparency over activities in cyber. For instance, agreements to notify each other if either is attacked in cyberspace against critical infrastructure could help to avert possible misunderstandings.Establish Norms for Responsible Cyber BehaviorBoth countries should adhere to international norms and frameworks for responsible behavior in cyberspace to avoid escalation and promote peace.•Adopt International Cyber Norms:The Governments of India and Pakistan should commit to international pacts on cyber norms as the UN "Group of Governmental Experts" (GGE) reports delineate aspects regarding state behavior in cyberspace. For example, it prohibits cyber intrusion in critical infrastructures or interference in one's internal matters.

International Mediation and Oversight: International bodies, such as the UN, can play a significant role in the mediation of disputes arising out of cyber attacks. The creation of a neutral body like the UN, or another equivalent organization, for cyber conflict resolution can develop an avenue to defuse cyber tensions at points just before they escalate to physical conflict.

Strenghten Regional Cooperation: Development of regional cooperation on cyber security initiatives: Both nations can work in participative programs for regional cyber security initiatives in the South Asian Association of Regional Cooperation (SAARC). It is also best in terms of establishing a platform of dialogue, cooperation, and exchange of information regarding cyber threats.Publish information about available effective services both governments must promote services that can remedy misinformation, as a way of aggressively countering it.

Awareness programs to the general population: Government and NGOs should educate people of the dangers of cyber attacks and disinformation. Educating the people about fake news, electronic intrusion, and online swindling may assist in shaping an emotionally aware and a more immune populace.

Joint exercises to curb disinformation: Pakistan and India can collaborate in finding out and stopping cross-border information attacks that are propagated through social media. The adoption of clear rules of engagements in the context of cyber warfare by the two nations and subsequent adherence by the two nations would help prevent the negative abject of online propaganda (Mustafa, Murtaza, Z., & Murtaza, 2020).

International Journal for Conventional and Non-Conventional Warfare

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

Cyber Warfare Rules of Engagement:Certain specific conditions upon which the countries would engage into cyberspace war should be well accepted and defined. Taking an example, they should not agree that cyber attack is permissible to attack civilian infrastructures or to further an already existing conflict.

Establish Red Lines in Cyber Warfare: pinpointing the notable area the term cyberattack is centered in a scenario involving an armed conflict, to include as well as measures that would attract a counter-reaction to a military response, would be effective in eliminating any likelihood of the same occurrence of such a phenomenon. An agreement should be arrived between the two countries on what constitutes cyber operations as an act of aggression.

Cyber Incident Reporting Centers: Develop communal and balancing Cyber Incident Response Teams (CIRTs) to report and react to cyber-assaults in real-time. False attribution or misapprehension can be avoided by information sharing before accidental escalation.

Policymaking: Collaboration in terms of policy can lead to a peaceful and stable digital environment where both countries can share non-sensitive cyber threat intelligence, and seek solutions to an apparently unstable digital environment

Trying to create such peaceful and cooperative atmosphere in the digital realm between the countries where they enjoy cooperation rather than hostility. After that, an example could be both India and Pakistan pursuing digital cooperation agreement that would give leeway to different joint development of technologies of synergies focused on cyber security measures so that they could roll out cooperative measures under the stake of digital governance. This kind of collaboration in the area of research in cyber security would bring new avenues to building of trust (O Hara, 2004).

Inclusive Internet Governance: Both countries should come together to join and work at the global regional level concerning the measures and control of the internet so open and safe while ensuring that malicious activities of cyber nature do not happen.

Conclusion

The ongoing cyber confrontation between India and Pakistan has elevated cyberspace from a peripheral issue to a central domain of strategic competition. Both states have progressively framed cyber threats as existential challenges to their sovereignty, national security, and critical infrastructure. This securitization has justified extraordinary measures such as the expansion of state surveillance, development of offensive cyber capabilities, and the establishment of dedicated cyber defense institutions. As a result, cyberspace has become militarized and politicized, with increasing emphasis on deterrence, retaliation, and control over digital narratives. The framing of cyberspace as a security threat rather than a cooperative or technical domain has significant implications. It fosters a climate of suspicion and opacity, in which each cyber incident—whether real, alleged, or misattributed risks triggering disproportionate responses. Moreover, the absence of mutual confidence-building mechanisms, regional cyber norms, or transparent dialogue exacerbates the potential for escalation and miscalculation. The digital domain's anonymity and deniability further complicate attribution and accountability, making it easier for hostile actions to occur under the threshold of open conflict. In this context, it becomes essential for both India and Pakistan to shift away from a purely securitized approach toward a more balanced and cooperative cyber posture. This includes initiating structured bilateral dialogues on cyber issues, adopting international norms for responsible state behavior in cyberspace, defining red lines around critical sectors, conducting joint cybersecurity exercises, and investing in public awareness

ISSN Online: 3078-2996, ISSN Print: 3078-2988

Volume No: 02 Issue No: 01 (2025)

campaigns to build digital resilience. Third-party mediation through international and regional platforms can also help reduce tensions and promote transparency. Without such efforts, the cyber domain will remain an unregulated battlefield amplifying mistrust, undermining regional stability, and increasing the risk that digital conflicts may spill over into traditional domains of warfare.

References

Aziz, M. (2020). Cybersecurity and digital sovereignty in Pakistan. Islamabad Policy Research Institute. https://ipripak.org

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Chaudhuri, R. (2021). India's cybersecurity challenges: Policy responses and emerging trends. Observer Research Foundation Occasional Paper Series, (341), 1–20. https://www.orfonline.org/research/indias-cybersecurity-challenges/

Deibert, R. (2013). The geopolitics of cyberspace after Snowden. Current History, 112(754), 9–15. https://doi.org/10.1525/curh.2013.112.754.9

Hussain, M., & Arshad, Z. (2022). Securitization of cyberspace in South Asia: The case of India-Pakistan rivalry. Journal of South Asian Strategic Studies, 8(2), 44–63.

Kavanagh, C., & Cowls, J. (2019). Cyber conflict and norms: Exploring the role of international law and multilateral agreements. Oxford Internet Institute. https://www.oii.ox.ac.uk

Lewis, J. A. (2019). Cybersecurity and stability in the global cyber domain. Center for Strategic and International Studies (CSIS). https://www.csis.org

Maitra, S. (2020). Offensive cyber capabilities and strategic stability in South Asia. Journal of Indo-Pacific Affairs, 3(4), 98–113. https://www.airuniversity.af.edu/JIPA/

Patil, D. A. (2021). Cybersecurity policy in India: Issues and challenges. Cybernomics, 3(5), 1–8. https://doi.org/10.5281/zenodo.4708225

Rasheed, A., & Rizwan, M. (2021). Cyber warfare and its implications for national security: A case study of Pakistan. Global Strategic and Security Studies Review, 6(1), 45–56. https://doi.org/10.31703/gsssr.2021(VI-I).05

Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Singh, R. (2020). Cyber conflict in South Asia: Challenges for Indian security. IDSA Monograph Series. https://idsa.in/monograph/cyberconflict-southasia

Tikk, E., Kaska, K., & Vihul, L. (2010). Cyber attacks against Georgia: Legal lessons identified. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org