Vol. 3 No.2 2025

RECOGNIZED IN "Y" CATEGORY BY

Research Consortium Archive

P(ISSN) : 3007-0031

E(ISSN) : 3007-004X

https://rc-archive.com/index.php/Journal/about

HYBRID WARFARE BETWEEN INDIA AND PAKISTAN: CYBER THREATS, DISINFORMATION, AND STRATEGIC STABILITY (2019–2024)

Dr. Dilawar Khan
Assistant Professor, Department of Political Science, Bacha Khan University Charsadda, KPK. dilawar1983@gmail.com
Wajid Mehmood
Assistant Professor, Political Science FATA University Dara Adam Khel, Kohat. wajid.mehmood@fu.edu.pk
Dr. Hassan Shah*
Assistant Professor & Head of the Department of Political Science, University of Buner. Corresponding Author Email: hassan_shah@ubuner.edu.pk

Publisher : EDUCATION GENIUS SOLUTIONS
Review Type: Double Blind Peer Review

ABSTRACT

This study explores the evolving landscape of hybrid warfare between India and Pakistan from 2019 to 2024, with a specific focus on cyber threats, disinformation campaigns, and their implications for strategic stability in South Asia. The research investigates how non-kinetic tools—such as cyberattacks, social media manipulation, and digital espionage—have supplemented conventional military posturing and contributed to a climate of persistent tension between the two nuclear-armed neighbors. Through qualitative and case-based analysis, it reveals the increasing sophistication of both states in employing hybrid tactics for political leverage, psychological impact, and international narrative control. The Pulwama-Balakot crisis, revocation of Article 370, and multiple cyber incidents serve as pivotal points to examine escalation dynamics. The study argues that while hybrid warfare provides new arenas of competition, it also exacerbates mistrust and destabilizes regional peace by blurring the lines between peace and conflict. The findings underscore the urgent need for bilateral confidence-building measures and multilateral frameworks to regulate hybrid threats and prevent escalation into full-scale conflict.

Keywords: Hybrid Warfare, India-Pakistan Relations, Cybersecurity, Disinformation, Strategic Stability, South Asia, Cyber Threats, Psychological Operations, Information Warfare, Escalation Dynamics

Introduction

The advent of hybrid warfare has significantly altered the strategic calculus between India and Pakistan, with both countries increasingly engaging in non-kinetic tactics to pursue their geopolitical interests without escalating to full-scale conventional war. Since the Pulwama-Balakot crisis in 2019, hybrid warfare has become a central element of India-Pakistan hostilities. Both states have employed tactics such as cyber intrusions, disinformation campaigns, and digital espionage to undermine each other’s internal stability and influence international narratives. For instance, Indian media and state-linked networks have accused Pakistan-based actors of launching cyber-attacks against critical Indian infrastructure, while Pakistan has similarly attributed cyber intrusions to Indian state-sponsored entities. These developments reflect a shift from traditional military confrontations to a more covert, persistent form of competition that operates across the cyber and information domains. This trend aligns with global patterns in contemporary warfare, where state and non-state actors increasingly leverage hybrid tactics to achieve asymmetric advantages without crossing the threshold of conventional warfare (Murray & Mansoor, 2012; Singh, 2021).

Cyber threats have emerged as a dominant tool in the hybrid strategies employed by India and Pakistan, particularly after 2019. Pakistan's cyber security infrastructure has reportedly been targeted by Indian-sponsored malware, phishing campaigns, and surveillance spyware, especially during periods of political instability. Simultaneously, Indian institutions, including power grids and defense websites, have suffered cyber-attacks that were allegedly traced to actors based in Pakistan or linked to groups with Pakistani affiliations. This cyber offensive-defensive exchange reflects a growing regional arms race in cyberspace, where state agencies are building capacities not only for defense but also for preemptive and retaliatory cyber strikes. These activities raise serious concerns about the risks of unintended escalation, especially in a nuclearized context where misattribution or disproportionate response could have grave consequences. Moreover, the absence of a comprehensive cyber confidence-building framework between India and Pakistan further intensifies the dangers posed by digital hostilities (Kavanagh et al., 2020; Ahmad, 2022).

Another significant dimension of hybrid warfare between India and Pakistan is the use of disinformation and psychological operations to influence public opinion and destabilize the adversary's internal environment. Social media platforms, such as Twitter, Facebook, and YouTube, have become battlegrounds where state-sponsored propaganda, fake news, and deepfake content are weaponized to polarize societies and promote hostile narratives. India has accused Pakistan of orchestrating social media disinformation campaigns targeting Indian elections, Kashmir-related issues, and communal tensions. Conversely, Pakistan has identified hundreds of fake websites and media outlets allegedly operated by Indian networks to discredit Pakistan internationally, as highlighted in the EU DisinfoLab's 2020 report. These information warfare tactics erode public trust, inflame nationalist sentiments, and blur the lines between truth and manipulation, making conflict resolution even more elusive. The growing sophistication of these operations highlights the urgency of developing regulatory mechanisms, bilateral codes of conduct, and international norms to manage the psychological front of hybrid warfare (EU DisinfoLab, 2020; Qureshi, 2023).

Theoretical Framework

The concept of hybrid warfare between India and Pakistan can be effectively analyzed through the lens of Hybrid Warfare Theory, which emphasizes the fusion of conventional, irregular, and cyber tactics in modern conflicts. This theory, popularized by military scholars such as Frank G. Hoffman, contends that hybrid threats are posed by both state and non-state actors who simultaneously employ political warfare, cyber operations, disinformation, and military force to exploit vulnerabilities across multiple domains. In the context of India and Pakistan (2019–2024), hybrid warfare theory explains how both nations have leveraged cyber-attacks, media manipulation, and psychological operations alongside conventional military posturing to gain strategic advantage without crossing into full-scale war. For instance, India’s cyber responses post-Pulwama and Pakistan’s narrative-building on Kashmir across digital platforms are hybrid tactics aimed at undermining each other's strategic coherence. Thus, hybrid warfare theory provides a critical framework for understanding how both nations navigate conflict in an era of digitally-driven geopolitical rivalry.

Literature Review

The concept of hybrid warfare has gained substantial attention in strategic and security studies over the past two decades. Frank G. Hoffman (2007) introduced the term to describe the blending of conventional, irregular, and cyber tactics by both state and non-state actors to achieve strategic objectives. According to Hoffman, hybrid warfare is not a new form of conflict but a modern manifestation of combined and coordinated strategies used to exploit an adversary’s weaknesses across multiple domains. The relevance of this concept has grown in recent years as technological advancement and digital communication have enabled new forms of aggression—most notably cyber-attacks and information manipulation—without traditional military engagement. Scholars emphasize that hybrid warfare is particularly suited for asymmetric environments where full-scale war is neither feasible nor desirable due to political, economic, or nuclear constraints. This theoretical framing has been instrumental in analyzing conflicts in the Middle East, Ukraine, and more recently, South Asia, (Hoffman, F. G. 2007).

In the South Asian context, researchers have increasingly applied the hybrid warfare framework to the Indo-Pakistani conflict, especially after 2019. C. Christine Fair (2019) notes that both India and Pakistan have diversified their strategic toolkits by incorporating non-kinetic operations such as cyber warfare and disinformation into their broader national security strategies. After the Pulwama-Balakot crisis, analysts observed a significant uptick in cyber threats and state-sponsored narratives aimed at discrediting the adversary domestically and internationally. Several Indian think tanks have argued that Pakistan’s Inter-Services Public Relations (ISPR) division has mastered the use of psychological operations via social media, while Pakistani analysts have accused Indian intelligence of running extensive disinformation networks, as exposed by the 2020 EU DisinfoLab investigation. The literature clearly shows an increasing focus on the “grey zone” of conflict where hybrid threats have become normalized and strategically effective (Fair, C. C. 2019)

Cyber security literature further reinforces the relevance of hybrid warfare in the Indo-Pakistani rivalry. According to Ahmad (2022), cyber-attacks have moved from isolated incidents to sustained campaigns involving data theft, surveillance, and disruption of essential services. Pakistan’s National Response Centre for Cyber Crimes (NR3C) has reported numerous intrusions from Indian-linked IP addresses, targeting government and military infrastructure. Similarly, India's Computer Emergency Response Team (CERT-IN) has flagged Pakistani-origin cyber-attacks, particularly those tied to periods of heightened geopolitical tension. Cyber security firms such as Fire Eye and Kaspersky have documented espionage campaigns, including phishing attacks and malware deployments, allegedly originating from both sides. This indicates the formalization of cyber capabilities as instruments of national policy. Scholarly work by Kavanagh et al. (2020) warns that without cyber security agreements or confidence-building measures, the potential for miscalculation in the cyber domain could destabilize the broader strategic environment in South Asia (Ahmad, T. 2022)

Disinformation and psychological operations are emerging themes in the literature on hybrid warfare, with growing recognition of their strategic utility. Qureshi (2023) highlights that disinformation is increasingly being used to manipulate public sentiment, influence elections, and distort policy debates. In Pakistan, anti-India narratives often dominate state and social media, while Indian media has been accused of promoting hyper-nationalist content that dehumanizes Pakistanis. These narratives, when repeated and amplified, shape public opinion and policymaking in ways that reduce the scope for dialogue and compromise. The weaponization of information—through fake news, bots, deepfakes, and manipulated videos—is identified as a deliberate strategy designed to sow confusion and mistrust. Scholars like Rid (2020) and Pamment (2017) argue that disinformation is not merely a propaganda tool but a form of strategic communication that can degrade democratic institutions and international diplomacy. This literature underscores the growing consensus that information warfare is a central pillar of hybrid warfare in the India-Pakistan context (Qureshi, A. M. 2023).

Problem Statement

From 2019 to 2024, India and Pakistan have increasingly engaged in hybrid warfare, marked by cyber threats, disinformation, and psychological operations. These non-traditional tactics have intensified mistrust, undermined strategic stability, and blurred the line between war and peace. The growing use of cyber-attacks and digital propaganda has created new security challenges that traditional diplomatic and military frameworks struggle to address. This study aims to explore how these hybrid tactics affect regional stability and conflict resolution efforts in South Asia.

Research Objectives

1. To critically analyze the impact of hybrid warfare—specifically cyber threats and disinformation campaigns—on strategic stability and bilateral relations between India and Pakistan from 2019 to 2024.

Research Questions

1. How have cyber threats and disinformation campaigns as instruments of hybrid warfare influenced strategic stability and

escalated tensions between India and Pakistan from 2019 to 2024?

Methodology

This study adopts a qualitative research approach using case study analysis.

Data Collection

Secondary Data will be collected from official documents, academic journals, news reports, and cyber security databases.

Data Analysis

Thematic analysis will be employed to identify patterns and interpret the impact of hybrid warfare tactics on India-Pakistan strategic stability.

Significance of the Study

This study highlights the growing threat of hybrid warfare in shaping regional security dynamics between India and Pakistan. It provides insights into how cyber threats and disinformation campaigns destabilize strategic balance without conventional warfare. The research contributes to understanding non-traditional security challenges in South Asia. Policymakers and defense strategists can benefit from its findings to craft informed responses. Ultimately, it promotes the need for regional cooperation and regulatory frameworks in the digital security domain.

Background of Hybrid Warfare

Hybrid warfare is a modern strategy that blends conventional military power with irregular tactics, cyber operations, disinformation, and psychological manipulation. It is designed to achieve strategic objectives without triggering open warfare. The concept gained prominence after its effective use by Russia in Crimea and Eastern Ukraine, prompting global awareness of non-traditional warfare domains. Hybrid warfare exploits the vulnerabilities of state institutions, media, and digital infrastructure to destabilize opponents while maintaining plausible deniability. It challenges traditional notions of conflict, necessitating new frameworks for defense and diplomacy (Hoffman, 2007).

Evolution of India-Pakistan Conflict Dynamics

India and Pakistan have shared a long history of conflict since their independence in 1947, marked by multiple wars, skirmishes, and enduring territorial disputes—especially over Kashmir. Traditionally, these confrontations were defined by conventional military engagements and nuclear deterrence post-1998. However, since the 2000s, the nature of conflict has evolved, incorporating proxy warfare, cyberattacks, and disinformation campaigns. The Pulwama-Balakot episode in 2019 and subsequent digital hostilities marked a shift toward hybrid conflict, illustrating how state and non-state actors now operate in a blurred conflict continuum. The South Asian region, due to its nuclear backdrop, historical animosities, and fragile political systems, is highly susceptible to hybrid tactics. Understanding the role of hybrid warfare in South

Asia is critical, as it allows scholars and policymakers to identify emerging threats that could destabilize regional peace without outright war. Studying hybrid tactics also helps in anticipating gray-zone conflicts—those that fall below the threshold of war but are deeply destabilizing. For India and Pakistan, hybrid threats not only influence military doctrines but also domestic politics, foreign policy, and regional diplomacy (Jones, 2018).

Definition and Dimensions of Hybrid Warfare

Hybrid warfare encompasses a strategic mix of kinetic and non-kinetic tools, including cyber-attacks, propaganda, economic pressure, and use of proxies. It aims to create ambiguity, confusion, and internal dissent within the targeted state. This warfare is conducted across multiple domains—land, air, sea, cyber, and information—and often avoids direct attribution. Unlike traditional warfare, hybrid strategies leverage technology, social media, and legal systems to create asymmetry and disrupt the adversary without crossing the threshold into open conflict. Conventional threats involve direct military confrontation using armed forces and are governed by established laws of war. Cyber threats, on the other hand, are digital intrusions targeting information systems, infrastructure, and private data, often launched anonymously. Hybrid threats combine these domains with irregular warfare, propaganda, and legal warfare to achieve political or military aims indirectly. The hybrid approach is more flexible and elusive, making it difficult for traditional military responses to effectively counter them (Kello, 2013).

The Role of Disinformation and Cyber Tools in Statecraft

Disinformation and cyber tools have become crucial instruments in modern statecraft, allowing states to manipulate narratives, distort public opinion, and create political instability in rival nations. Social media platforms are often weaponized to spread fake news, promote extremist ideologies, and deepen social divisions. Cyber espionage targets critical infrastructure, defense systems, and government data, weakening state capacity and resilience. In the India-Pakistan context, both sides have engaged in such tactics to shape domestic and international perceptions, particularly after events like the Balakot airstrikes and the abrogation of Article 370. Strategic stability refers to the absence of incentives for any side to alter the status quo through force, especially in nuclear-armed rivalries like India and Pakistan. Asymmetric warfare, which includes hybrid tactics, threatens this stability by creating security dilemmas and eroding mutual trust. Classical deterrence theory struggles to address these new tactics because hybrid operations often remain below the threshold of military retaliation. This leads to escalation risks, particularly in a volatile region where misperceptions and rapid responses can have severe consequences (Waltz, 1981).

Relevance to South Asia

Hybrid warfare is particularly relevant to South Asia, a region marked by historical rivalries, fragile democracies, and rapid digitalization. India and Pakistan’s hybrid conflict highlights how modern statecraft is evolving in high-risk, nuclear-armed regions. Understanding hybrid threats in South Asia is essential for regional stability, as these tactics exploit ethnic tensions, political instability, and weak cyber regulations. This study contributes to identifying mechanisms for crisis prevention, confidence-building, and digital diplomacy in one of the world’s most volatile regions (Fair, 2014).

Pre-2019 Strategic Environment

Before 2019, the strategic environment between India and Pakistan was characterized by a fragile balance of power, underpinned by the doctrine of nuclear deterrence. Since the nuclear tests of 1998, both countries maintained a policy of avoiding full-scale war, relying instead on low-intensity conflicts, proxy warfare, and diplomatic maneuvering. Despite repeated crises, such as the Kargil War (1999) and the Mumbai attacks (2008), both nations avoided escalation beyond a certain threshold due to the looming threat of nuclear retaliation. However, during this period, the seeds of hybrid warfare—such as information manipulation, cyber espionage, and cross-border ideological influence—began to take root. The absence of formal arms control agreements or robust crisis communication mechanisms made the environment precarious, with even minor incidents having the potential to spiral into larger confrontations. (Kapur, 2008).

Legacy of Kargil, Mumbai Attacks, and Uri Strikes

The Kargil War of 1999, initiated by Pakistani forces and militants occupying Indian posts in Kashmir, fundamentally altered perceptions of deterrence and trust between the two nations. Although India successfully repelled the incursion, the war showed that limited conventional war could still occur under the nuclear umbrella. The 2008 Mumbai attacks marked another shift, where a non-state group allegedly supported by elements within Pakistan’s security establishment conducted a high-profile terrorist operation in India’s financial capital. This event brought global condemnation and strained diplomatic ties to their breaking point. Later, in 2016, the Uri attacks where 19 Indian soldiers were killed—provoked a significant Indian military response in the form of cross-border “surgical strikes,” signaling a shift in Indian doctrine from strategic restraint to active retaliation. These incidents left a lasting legacy of mistrust and underscored the need for new defense paradigms beyond conventional war (Tellis, 2001; Pant, 2016).

Traditional vs. Non-traditional Warfare Tactics

Traditional warfare, which involves direct confrontation between state militaries, is governed by established doctrines, laws of armed conflict, and visible consequences. In contrast, non-traditional or hybrid warfare incorporates tools like cyber-attacks, disinformation, economic coercion, and the use of non-state actors. These tactics allow states to operate in the "gray zone," below the threshold of war, making attribution difficult and response complicated. In the India-Pakistan context, while traditional warfare dominated the 20th century, the 21st century has seen a significant shift toward non-traditional threats. For instance, cyber-attacks on critical infrastructure and coordinated media misinformation campaigns have emerged as significant concerns post-2016. The blending of these tactics complicates defense responses and requires a redefinition of what constitutes aggression in modern statecraft (Hoffman, 2007; Renz, 2016).

Influence of Global Actors (US, China, Russia) on South Asian Security

The strategic environment in South Asia is heavily influenced by the involvement of global powers, notably the United States, China, and Russia. The United States has traditionally played the role of crisis manager, particularly during India-Pakistan conflicts, aiming to de-escalate tensions and maintain regional stability. However, its tilt toward India in recent years through defense agreements and the Quad alliance has raised concerns in Pakistan. China, on the other hand, has deepened its strategic and economic ties with Pakistan through the China-Pakistan Economic Corridor (CPEC), while maintaining complex border tensions with India. This triangular relationship adds to the security dilemmas in South Asia. Russia, historically aligned with India, has started diversifying its ties, selling arms to both India and Pakistan and promoting a multi-vector diplomacy. These dynamics reflect a multipolar influence on regional conflicts, often acting as force multipliers for hybrid tactics, particularly in cyber and information warfare (Joshi, 2021; Small, 2015).

Notable Cyber Attacks on Critical Infrastructure (Government, Military, Finance)

From 2019 to 2024, both India and Pakistan have experienced significant cyber-attacks targeting critical infrastructure. In India, the 2020 cyber-attack on the Mumbai power grid—allegedly linked to Chinese and possibly Pakistani actors—disrupted power supply in the financial capital, raising concerns about the vulnerability of India’s cyber-physical systems. Similarly, Pakistan has faced repeated breaches of its governmental and military networks. In 2021, reports revealed that Indian actors deployed spyware and phishing campaigns against Pakistani military officials and nuclear scientists, aiming to extract strategic information. Financial institutions in both countries have also been victims of ransomware and data theft, indicating the increased use of cyber tools in hybrid warfare. These incidents underscore how digital infrastructure has become a frontline in strategic competition (Bhatt, 2021; Gupta, 2022).

Attribution Challenges and Proxy Actors

One of the defining features of cyber conflict is the challenge of attribution—accurately identifying the perpetrator behind an attack. In the South Asian context, both India and Pakistan face difficulties in proving state responsibility due to the use of third-party actors, non-state hackers, and false-flag operations. Groups like APT36 (believed to be Pakistan-based) and SideWinder (linked to India) have conducted cyber-espionage campaigns while maintaining plausible deniability for their respective governments. This ambiguity allows states to engage in cyber operations without triggering conventional retaliation, making it a preferred tool in hybrid warfare. The use of proxy actors also complicates international legal responses, as the lines between criminal and strategic intent blur significantly in cyberspace (Rid & Buchanan, 2015; Clarke & Knake, 2019).

Role of Indian and Pakistani State-sponsored Cyber Units

Both India and Pakistan have developed cyber units integrated into their military and intelligence frameworks. India's Defence Cyber Agency (established in 2019) operates under the Ministry of Defence, tasked with offensive and defensive cyber operations. It collaborates with other intelligence agencies to monitor, disrupt, and deter cyber threats. Pakistan's Inter-Services Intelligence (ISI) and Army Cyber Command also maintain cyber capabilities, primarily focusing on surveillance, information operations, and disruption of Indian networks. These units are believed to support influence campaigns, especially during periods of heightened tension such as elections or after major attacks like Pulwama. While these agencies provide a degree of strategic cyber deterrence, their operations remain largely covert and are seldom acknowledged officially, preserving operational ambiguity (Tikk et al., 2017; Sharma, 2020).

Cyber Security Policies and Doctrinal Shifts in Both States

India and Pakistan have begun formalizing their approaches to cyber security through policy and doctrinal developments. India released the "National Cyber Security Policy" in 2013 and has since updated its frameworks to include public-private partnerships, critical infrastructure protection, and AI integration. Meanwhile, the Draft National Cyber Security Strategy of 2021 aims to build a robust defense mechanism against cyber threats. Pakistan introduced its first Cyber Crime Act in 2016, followed by a National Cyber Security Policy in 2021, focusing on institutional coordination and military preparedness. Both nations are gradually shifting their doctrines to recognize cyberspace as a domain of warfare, comparable to land, air, and sea. This doctrinal evolution reflects a growing understanding that cyber capabilities are essential for national defense and geopolitical competition (Kaplan, 2016; Khan, 2022).

Regional and Global Responses to Cyber Escalation

The increasing cyber tensions between India and Pakistan have not gone unnoticed by regional and global actors. The United States, through its Indo-Pacific strategy, has promoted cyber security cooperation with India, offering technical assistance and intelligence-sharing. China, while remaining neutral on Indo-Pak cyber issues, has deepened digital ties with Pakistan through joint projects like CPEC's digital backbone. International organizations like the UN and ITU have called for cyber norms and confidence-building measures (CBMs) in South Asia to prevent miscalculations. ASEAN and the SCO have also provided platforms for cyber dialogue, though progress remains limited. Overall, while regional cooperation on cyber governance is still in its infancy, global actors increasingly view South Asia's cyber conflict as a flashpoint that could escalate into broader instability (Maurer, 2018; Singh & Bhatnagar, 2021).

Disinformation Campaigns and Psychological Warfare

1. Media Manipulation, Troll Armies, and Bot Networks

In the digital landscape of South Asia, particularly between India and Pakistan, media manipulation has evolved as a prominent tool of hybrid warfare. State and non-state actors deploy troll armies and automated bot networks to amplify polarizing content, harass dissenters, and control narratives. These troll factories are often state-supported or linked to political interests, generating hashtags and memes to manufacture consent or discredit opponents. Bot networks are capable of simulating public consensus, misleading international observers and domestic audiences. Such manipulation has contributed to the hardening of nationalistic sentiments and the erosion of critical journalism. Troll armies on both sides have been accused of inflaming ethnic and sectarian tensions, further destabilizing the region's socio-political fabric (Bradshaw & Howard, 2018).

2. Use of Fake News during Cross-Border Crises (e.g., Pulwama, Balakot &Article 370)

Cross-border crises between India and Pakistan have frequently seen a surge in disinformation and fake news. Following the Pulwama attack in 2019, both countries engaged in a digital battle to control the narrative. In India, social media and mainstream outlets circulated unverified reports on the number of casualties inflicted during the Balakot airstrike, while in Pakistan, online platforms sought to disprove those claims and promote counter-narratives. Similarly, after the abrogation of Article 370, misinformation about the situation in Jammu and Kashmir spread across social media platforms, with conflicting visuals and videos often taken out of context. These episodes reveal how fake news intensifies conflict, reduces space for diplomacy, and fuels hostility between already tense neighbors (Farooq, 2020).

3. Role of Social Media Platforms (Facebook, X/Twitter, WhatsApp, YouTube)

Social media platforms have become central arenas in shaping political discourse and conducting hybrid warfare in South Asia. Facebook, X (formerly Twitter), WhatsApp, and YouTube are routinely exploited to spread propaganda, incite hatred, and mobilize public sentiment. Coordinated inauthentic behavior, such as fake profiles and orchestrated campaigns, has been documented on both Indian and Pakistani sides. WhatsApp, in particular, is a powerful vector for misinformation due to its encrypted, peer-to-peer nature, making it difficult to monitor or correct false narratives. While platforms have occasionally removed problematic content or accounts, their responses have often been reactive rather than proactive, allowing disinformation to thrive during critical geopolitical events (Kaur & Zayani, 2021).

4. Public Opinion, Perception Management, and Electoral Influence

Digital disinformation campaigns have significantly influenced public opinion and electoral outcomes in both India and Pakistan. Political actors utilize data-driven techniques, often borrowed from foreign models like Cambridge Analytica, to target voters with customized propaganda. In India, the BJP has been accused of managing vast IT cells that shape political discourse and suppress criticism online. In Pakistan, political parties and security institutions are believed to manipulate online sentiment through fake accounts and influencer partnerships. This manipulation skews democratic processes, delegitimizes opposition, and consolidates power under the guise of popular support. The result is a digitally manufactured consensus that undermines the principles of free speech and informed political participation (Patel & Kumar, 2022).

5. Impact on National Unity and Diplomatic Relations

The weaponization of information has had a corrosive impact on national unity and interstate diplomacy. Internally, fake news and divisive content aggravate ethnic, religious, and regional divides, particularly in fragile areas like Kashmir or Balochistan. Nationalist rhetoric and conspiracy theories reduce public trust in institutions and breed intolerance, weakening the social fabric. Externally, misinformation campaigns disrupt backchannel diplomacy and increase the likelihood of miscalculation during crises. False flag operations, doctored videos, and strategic leaks are now part of the diplomatic toolkit, eroding traditional norms of engagement. This undermines efforts at peace-building and trust, replacing dialogue with digital hostility (Chaudhuri, 2021).

Strategic Stability under Hybrid Pressure

1. Impact of Hybrid Warfare on Deterrence Dynamics

Hybrid warfare combining cyber-attacks, disinformation campaigns, and irregular tactics has significantly altered traditional deterrence between India and Pakistan. While nuclear deterrence previously maintained a fragile peace, hybrid methods have allowed low-level provocations without triggering full-scale conflict. These "gray zone" tactics complicate attribution and response, thus blurring red lines and weakening the credibility of deterrence strategies. As both countries adopt non-traditional tools, the balance of power becomes increasingly unpredictable, raising concerns over strategic miscalculations and escalation (Raska, M. 2020).

2. Crisis Escalation Management (e.g., 2019 Air Strikes, Border Skirmishes)

The 2019 Pulwama-Balakot episode illustrated how hybrid warfare affects crisis escalation management. While both nations exercised some level of restraint to avoid nuclear confrontation, the speed and spread of misinformation online inflamed public opinion, reducing policy space for de-escalation. Border skirmishes, amplified by aggressive media narratives and social media, make managing escalation increasingly complex. Quick political decisions, often influenced by popular sentiment, can override diplomatic channels (Ganguly, Š., & Scobell, A. 2019).

3. Nuclear Signaling Amid Cyber and Disinformation Threats

Cyber intrusions and disinformation campaigns obscure nuclear signaling, a critical component of strategic stability. In the past, overt signals like missile tests or military deployments were used to convey deterrent intent. Today, false narratives, deepfakes, and hacking attempts risk misinterpretation of nuclear posture or command intent. This ambiguity heightens the danger of accidental or unauthorized escalation, especially in the absence of robust communication mechanisms (Krepon, M. 2021).

4. The Role of External Powers and Multilateral Forums in Conflict Mediation

External actors like the United States, China, and Russia, along with multilateral institutions like the United Nations, play a pivotal role in mediating India-Pakistan tensions, particularly during crises involving hybrid threats. These actors often provide backchannel diplomacy, issue de-escalation appeals, or impose normative pressure. However, their effectiveness is limited by geopolitical interests and a lack of unified frameworks for managing hybrid threats in South Asia (Bajpai, K. 2021)

5. Policy Gaps in Strategic Communication and Trust-building

Despite repeated crises, both India and Pakistan lack coherent policies for strategic communication during hybrid conflicts. Misunderstandings are often exacerbated by nationalistic media and cyber propaganda. Confidence-building measures (CBMs) remain outdated and underutilized in addressing cyber norms or disinformation. The absence of crisis hotlines for digital threats, shared incident reporting, and formal mechanisms for cyber deterrence presents a critical gap in maintaining regional peace (Panda, A. 2020)

Case Studies and Empirical Analysis

Case Study 1: Pulwama–Balakot Crisis (2019)

The Pulwama–Balakot crisis marked a watershed in India-Pakistan relations and was heavily influenced by hybrid warfare strategies. The suicide bombing in Pulwama, Jammu & Kashmir, on February 14, 2019, which killed 40 Indian paramilitary personnel, was followed by India's airstrike in Balakot, Pakistan, allegedly targeting a Jaish-e-Mohammed training camp. This incident was not only a military exchange but also a digital conflict, as both nations launched intensive information campaigns online. The spread of exaggerated casualty figures, patriotic hashtags, fake news, and conflicting official narratives created confusion and inflamed nationalistic sentiments on both sides. The crisis demonstrated how misinformation and cyber operations can escalate tensions and complicate de-escalation efforts (Ganguly, Š., & Scobell, A. 2019)

Case Study 2: Article 370 Revocation and Cyber Narratives

On August 5, 2019, the Indian government revoked Article 370, stripping Jammu and Kashmir of its semi-autonomous status. The move sparked a massive cyber narrative war between India and Pakistan. India imposed a prolonged internet blackout in the region to control unrest, while Pakistan launched an aggressive diplomatic and digital campaign to highlight alleged human rights violations. Social media platforms were flooded with coordinated hashtags, fake images, and international lobbying efforts. Disinformation campaigns were launched to influence global public opinion and discredit opposing narratives. This cyber component significantly shaped the international response to the crisis and intensified mutual mistrust (Farooq, U. 2020)

Case Study 3: Cross-border Disinformation during Elections

Both India and Pakistan have faced increasing levels of foreign interference and disinformation during their national elections. Troll farms, fake news pages, and bot networks have attempted to sway voter opinion, spread conspiracy theories, and delegitimize opposition leaders. In India, reports have emerged of online campaigns targeting Muslim minorities and linking them with Pakistan-based threats to consolidate majoritarian support. Conversely, in Pakistan, Indian-linked social media handles have attempted to discredit military institutions and political figures. These digital campaigns erode electoral integrity and weaken democratic resilience by manipulating public perception at critical political moments (Patel, A., & Kumar, N. 2022).

Expert Interviews and Data from Think Tanks (ORF, ISSI, SIPRI, etc.)

Expert interviews and research from leading think tanks like the Observer Research Foundation (ORF), Institute of Strategic Studies Islamabad (ISSI), and Stockholm International Peace Research Institute (SIPRI) offer valuable insights into the strategic implications of hybrid warfare. These sources analyze defense spending trends, cyber capabilities, regional perceptions, and emerging security doctrines. For instance, ORF reports highlight India's push for integrated cyber commands, while ISSI discusses Pakistan’s digital diplomacy in countering India’s narratives. SIPRI’s data is instrumental in evaluating military capacities and the role of technological innovation in shaping future conflicts. Such institutional analyses enhance the academic credibility and policy relevance of hybrid warfare studies (SIPRI. 2022).

Content Analysis of Social Media Trends and Campaigns

Content analysis of social media trends between 2019 and 2024 reveals a clear weaponization of platforms like Twitter (now X), Facebook, and YouTube for strategic purposes. Campaigns such as Boycott Pakistan, Stand with Kashmir, and Balakot Strikes were part of orchestrated digital operations often supported by bots and fake profiles. Hashtag activism, viral misinformation, and emotionally charged visuals were used to rally domestic support and discredit the opponent. Such analysis uncovers patterns of narrative control, sentiment manipulation, and timing that coincide with geopolitical developments, indicating strategic intent behind social media operations. Tools like sentiment analysis software and bot detection algorithms have been used to trace and decode these digital footprints (Kaur, R., & Zayani, M. 2021).

Pakistan's and India's Cyber Security and Information Warfare Strategies

India and Pakistan have both evolved their cyber security and information warfare strategies significantly in recent years, especially amid growing regional instability and technological advancement. India has taken active steps to strengthen its cyber command under the Defence Cyber Agency, which focuses on both defensive and offensive cyber capabilities. It has also embraced doctrines emphasizing information dominance in times of conflict. On the other hand, Pakistan has developed a National Cyber Security Policy (2021), focusing on national security, infrastructure protection, and digital sovereignty. Pakistan's Inter-Services Public Relations (ISPR) and India's Information Warfare Division within the armed forces play leading roles in perception management and online influence campaigns. Both countries have utilized social media for narrative building, psychological operations, and propaganda, blurring the lines between peace and war (Singh, R. (2021).

Confidence Building Measures (CBMs) and Hotlines

Confidence-building measures (CBMs) have historically played a vital role in diffusing tensions between India and Pakistan, especially regarding nuclear and military crises. In the realm of cyber and information warfare, however, CBMs are still rudimentary. Traditional military hotlines do exist—such as those between the Directors-General of Military Operations (DGMO)—but they are rarely used to discuss cyber incidents or disinformation campaigns. Experts have called for expanding CBMs to include digital transparency, notification mechanisms for cyber incidents, and collaborative threat assessments to reduce miscalculation risks. Establishing cyber hotlines and data-sharing protocols could help mitigate the impact of hybrid threats (Ahmed, M. (2020).

Role of Track II Diplomacy and Media Ethics Codes

Track II diplomacy—informal dialogue involving academics, retired officials, journalists, and civil society—plays a critical role in addressing contentious issues like hybrid warfare, where formal diplomatic channels may falter. Institutions such as the Regional Centre for Strategic Studies (RCSS) and the Institute of Peace and

Conflict Studies (IPCS) have facilitated such engagements, focusing on information ethics, media responsibility, and cyber conflict resolution. Furthermore, regional media councils and journalist unions have proposed ethical codes to counter disinformation and promote responsible reporting during crises. These efforts aim to reduce the inflammatory role of media and create space for dialogue rather than confrontation (Rizvi, H. (2021).

How to Maintain Strategic Stability

Strategic stability between India and Pakistan hinges on the ability to manage crises, communicate clearly, and deter conflict escalation—especially in the face of hybrid threats. A multidimensional approach is essential: strengthening institutional capacities for cyber defense, establishing formal communication protocols for cyber incidents, and reinforcing legal norms through international cooperation. Dialogue must also be enhanced via Track I and Track II channels, alongside promoting cyber CBMs. Most importantly, both nations must invest in digital literacy, media regulation, and de-escalation mechanisms that can neutralize the destabilizing effects of disinformation and cyber warfare (Krepon, M. (2021).

Conclusion

The evolving nature of hybrid warfare between India and Pakistan—characterized by cyber threats, disinformation campaigns, and psychological operations—has added a new dimension to their longstanding rivalry. Traditional military strategies are no longer sufficient to ensure strategic stability, as emerging technologies and digital platforms increasingly shape public perception, crisis escalation, and deterrence dynamics. State-sponsored cyber units, the manipulation of social media, and the lack of clear legal frameworks make the region more vulnerable to miscalculations and unintended conflict escalation. To maintain regional peace and security, both India and Pakistan must adopt a multi-pronged strategy that includes strengthening cyber security infrastructure, enhancing media literacy, and promoting bilateral cyber confidence-building measures. The role of Track II diplomacy, ethical media practices, and international legal norms such as the Tallinn Manual is increasingly vital in managing hybrid threats and avoiding full-scale conflict. As the region continues to navigate an unstable security environment, adapting to the realities of hybrid warfare is not just a strategic necessity—it is a prerequisite for long-term peace and coexistence.

Findings

1. Cyber operations have become a central element of India-Pakistan hybrid warfare post-2019.
2. Disinformation campaigns significantly influence public perception and escalate bilateral tensions.
3. Attribution of cyber-attacks remains difficult, encouraging proxy actors and plausible deniability.
4. State-sponsored cyber units in both countries play a growing

role in strategic communication and deterrence.

5. Existing confidence-building measures do not adequately address cyber and informational threats.
6. Social media manipulation during crises (e.g., Pulwama, Balakot) shapes electoral and diplomatic outcomes.
7. International legal frameworks are underdeveloped, creating regulatory vacuums in cyber conflict management.
8. Track II diplomacy and ethical media practices are essential to reduce hybrid escalation risks.

Recommendations

1. Establish bilateral cyber confidence-building measures to reduce misperceptions and crisis escalation.
2. Develop joint protocols for cyber incident reporting and crisis communication between India and Pakistan.
3. Promote regional agreements aligned with international norms like the Tallinn Manual to regulate cyber conduct.
4. Strengthen digital literacy and media ethics frameworks to counter disinformation and manipulation.
5. Empower Track II diplomacy to facilitate dialogue on hybrid threats and foster mutual understanding.
6. Invest in secure cyber infrastructure and threat monitoring systems to enhance national resilience.
7. Encourage social media platforms to collaborate with states on curbing fake news during cross-border crises.
8. Integrate hybrid warfare scenarios into strategic stability and defense planning in South Asia.

References

Ahmad, T. (2022). The evolution of cyber warfare in South Asia: Strategic implications for Pakistan and India. *Asian Affairs*, 53(3), 371–389.

Ahmad, T. (2022). The evolution of cyber warfare in South Asia: Strategic implications for Pakistan and India. *Asian Affairs*, 53(3), 371–389.

Ahmed, M. (2020). Confidence-building in South Asia: Broadening the agenda. *SIPRI Policy Paper*, 57, 1–22. https://www.sipri.org/publications/2020/sipri-policy-papers/confidence-building-south-asia

Bajpai, K. (2021). External actors and strategic stability in South Asia. *Contemporary South Asia*, 29(2), 229–246.

Bhatt, S. (2021). India’s cyber vulnerabilities and the Mumbai power outage. *Observer Research Foundation*. Retrieved from https://www.orfonline.org

Bradshaw, S., & Howard, P. N. (2018). The global organization of social media disinformation campaigns. *Journal of International Affairs*, 71(1.5), 23–32.

Chaudhuri, R. (2021). Digital frontlines and diplomatic backchannels: Information warfare and peace in South Asia. *Strategic Analysis*, 45(1), 12–29.

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending*

Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin.

EU DisinfoLab. (2020). *Indian Chronicles: Deep dive into a 15-year influence operation.* https://www.disinfo.eu/publications/indian-chronicles

Fair, C. C. (2014). *Fighting to the End: The Pakistan Army's Way of War*. Oxford University Press.

Fair, C. C. (2019). *In Their Own Words: Understanding Lashkar-e-Tayyaba*. Oxford University Press.

EU DisinfoLab. (2020). *Indian Chronicles: Deep dive into a 15-year influence operation.* https://www.disinfo.eu/publications/indian-chronicles/

Farooq, U. (2020). Disinformation in South Asia: A digital battlefield between India and Pakistan. *Digital Journalism*, 8(10), 1245–1263.

Farooq, U. (2020). Disinformation in South Asia: A digital battlefield between India and Pakistan. *Digital Journalism*, 8(10), 1245–1263.

Ganguly, Š., & Kapur, S. P. (2010). *India, Pakistan, and the Bomb: Debating Nuclear Stability in South Asia*. Columbia University Press.

Ganguly, Š., & Scobell, A. (2019). Balakot and the future of crisis stability in South Asia. *Survival*, 61(6), 43–50.

Gupta, R. (2022). Cyber operations in South Asia: India's strategic response. *Cyber Defense Review*, 7(2), 58–71.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies. https://www.potomacinstitute.org

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics*, 22(3), 283–300.

Jones, S. G. (2018). *Waging Insurgent Warfare: Lessons from the Vietcong to the Islamic State*. Oxford University Press.

Joshi, S. (2021). *How India Sees the World: Kautilya to the 21st Century*. Harper Collins India.

Small, A. (2015). *The China–Pakistan Axis: Asia's New Geopolitics*. Oxford University Press.

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War*. Simon & Schuster.

Kapur, S. P. (2008). *Dangerous deterrent: Nuclear weapons proliferation and conflict in South Asia*. Stanford University Press.

Kaur, R., & Zayani, M. (2021). Digital platforms and the rise of information wars in South Asia. *Media, Culture & Society*, 43(6), 1021–1040.

Kaur, R., & Zayani, M. (2021). Digital platforms and the rise of information wars in South Asia. *Media, Culture & Society*, 43(6), 1021–1040.

Kavanagh, C., Efron, S., & Gartzke, E. (2020). *Cybersecurity and strategic stability in South Asia*. Carnegie Endowment for International Peace. https://carnegieendowment.org

Kavanagh, C., Efron, S., & Gartzke, E. (2020). *Cybersecurity and strategic stability in South Asia*. Carnegie Endowment for International Peace. https://carnegieendowment.org

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), 7–40. https://doi.org/10.1162/ISEC_a_00138

Khan, F. (2022). Pakistan's cyber policy: Between aspirations and capacity. *South Asian Voices*. Retrieved from https://southasianvoices.org

Khan, M. I. (2022). Pakistan's National Cyber Security Policy and the growing digital threat landscape. *ISSI Strategic Studies*, 42(1), 55–72. https://issi.org.pk

Krepon, M. (2021). Nuclear signaling in the digital age. *Arms Control Today*, 51(1), 14–20. https://www.armscontrol.org/act/2021-01/features/nuclear-signaling-digital-age

Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press.

Murray, W., & Mansoor, P. R. (2012). *Hybrid warfare: Fighting complex opponents from the ancient world to the present*. Cambridge University Press.

Murray, W., & Mansoor, P. R. (Eds.). (2012). *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. Cambridge University Press.

Pamment, J. (2017). *Countering disinformation: The case for strategic communication*. Swedish Civil Contingencies Agency.

Panda, A. (2020). Strategic communication and South Asian security: Bridging the trust deficit. *The Diplomat*. https://thediplomat.com/2020/03/strategic-communication-and-south-asian-security/

Patel, A., & Kumar, N. (2022). Weaponizing public opinion: Electoral disinformation and democracy in South Asia. *Asian Journal of Communication*, 32(4), 367–384.

Patel, A., & Kumar, N. (2022). Weaponizing public opinion: Electoral disinformation and democracy in South Asia. *Asian Journal of Communication*, 32(4), 367–384.

Qureshi, A. M. (2023). Disinformation as a tool of hybrid warfare: The India-Pakistan media front. *South Asian Journal of International Affairs*, 15(1), 54–78.

Qureshi, A. M. (2023). Disinformation as a tool of hybrid warfare: The India-Pakistan media front. *South Asian Journal of International Affairs*, 15(1), 54–78.

Raska, M. (2020). Strategic competition in the age of hybrid warfare. *Journal of Strategic Studies*, 43(7), 928–952.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of*

Strategic Studies, 38(1-2), 4–37.

Rizvi, H. (2021). The potential of Track-II diplomacy in South Asia. Journal of Peace building & Development, 16(1), 87–103

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Sharma, R. (2020). India's growing cyber capability: Challenges and policy needs. *Vivekananda International Foundation*. Retrieved from https://www.vifindia.org

Singh, R. (2021). India's evolving cyber capabilities. *Observer Research Foundation*. https://www.orfonline.org

Singh, R., & Bhatnagar, S. (2021). Cyber diplomacy in South Asia: A way forward. *Journal of International Affairs*, 74(1), 85–102.

Singh, S. (2021). Cyber conflict and hybrid warfare in South Asia: The emerging security dynamics between India and Pakistan. *Journal of Strategic Studies*, 44(2), 267–289.

SIPRI. (2022). Trends in world military expenditure, 2022. *Stockholm International Peace Research Institute*. https://www.sipri.org/publications/2022/sipri-fact-sheets/trends-world-military-expenditure-2022

ORF. (2020). India's cyber capabilities: Prospects and challenges. *Observer Research Foundation*. https://www.orfonline.org

ISSI. (2021). Hybrid warfare: Pakistan's response and strategic outlook. *Institute of Strategic Studies Islamabad*. https://issi.org.pk

Tellis, A. J. (2001). *India's emerging nuclear posture: Between recessed deterrent and ready arsenal*. RAND Corporation.

Pant, H. V. (2016). India's 'surgical strikes' and the new strategic calculus. *The Diplomat*. Retrieved from https://thediplomat.com

Thussu, D. K. (2020). Media ethics in South Asia: Addressing misinformation and propaganda. South Asian Journal of Global Media and Communication, 11(2), 111–125.

Tikk, E., Kaska, K., & Vihul, L. (2017). *International Cyber Incidents: Legal Considerations*. NATO CCD COE Publications.

Waltz, K. N. (1981). *The Spread of Nuclear Weapons: More May Be Better*. Adelphi Papers, International Institute for Strategic Studies.