CYBER-EQUATION BETWEEN INDIA AND PAKISTAN: PRETEXT OF STABILITY-INSTABILITY PARADOX

Ms. Ayesha Shaikh, Mr. Gulraiz Iqbal & Mr. Ammar Hassan Sajjad*

Abstract

Humanity has evolved over the centuries, inventing new offences and counter-defense, Cyber-security threats are one of the newly emerged challenges of the 21st century that the lessons of the past are unaccustomed to dealing with. India and Pakistan have a history of complex rivalry. However, adding the cyber-security threats into the matrix complicates it further. The research evaluates the impacts and prospects of the cyber-security equation between the two mutually deterred nuclear rivals. From the standpoint of the stability-instability paradox, the research has explained the strategic balance between the two states in general and in the domain of cyber-security in particular. Research is exploratory as it explores the linkage between two variables (The cyber-security equation and the stability-instability paradox). It follows a qualitative design and case-study method. Data has been obtained from secondary sources. Evidence presented in the paper suggests an increase in the number of cyber-attacks and counter-attacks between India and Pakistan, with an overall disturbance of the strategic balance. The hegemonic aspirations of India and the uncompromising defensive posture of Pakistan can pave the way for the rupture of cyber-brinkmanship into a nuclear escalation. Therefore, the study proposes that both states acknowledge the need to establish cyber-security regimes and take preventive measures to spare the future from the shadow of unseen wars.

Keywords: Cyber-Security, Stability-Instability Paradox, India, Pakistan, Brinkmanship, Strategic Balance

Introduction

On the 16th of June, 2023, a Cyber-attack was launched on National Institutional Facilitation Technology (NIFT) Pakistan[1]. The attack holds significance, as it revealed the extent of vulnerability of a Nuclear-weapon state to the prevalent unconventional threats. Pakistan and India, with a history of rivalry against the nuclear-armed neighbouring state, are on the quest to develop a cyber-security network before the rival exploits the delay. Evolution in the technology field has resulted in the emergence of myriad threats that the traditional strategic apparatus is unaccustomed to dealing with. Cyber-security falls under the domain of these modern challenges. Cyber-security is "The organisation and collection of resources, processes and structures used to protect cyberspace and cyberspace-enabled systems

*Ms. Ayesha Shaikh is Research Assistant at Strategic Vision Institute Islamabad. Mr. Gulraiz Iqbal is an independent researcher based in Islamabad. Mr. Ammar Hassan Sajjad is an M.Phil International Relations Scholar and Visiting Faculty member at International Islamic University, Islamabad. The authors' email address is gulraiziqbal08@outlook.com

from occurrences that misalign de jure from de facto property rights."[2] Humanity has evolved over the centuries, inventing new offences and counter-defenses. During the Cold War, for instance, nuclear weapon technology and its associated strategies were the disposition of the international system. Through half a century of the Cold War, states learned the art of co-existing in a Nuclear-armed world. Regimes and protocols were incepted to legitimise the developments and minimise the damage. Today's world strives to wrap its head around hybrid warfare; cyber-security is one crucial element. With these developments in place, the world must formulate new strategies and laws to govern these newly discovered horizons.

The lessons that the great wars and the Cold War handed down included the caution against a nuclear war. Stability-instability paradox is one of the many theoretical explanations for this phenomenon. It established that Nuclear-weapon states are mutually deterred. Therefore, Nuclear weapons have ensured the stability of the larger strategic balance between the nuclear-armed states. However, history has witnessed minor classes or conflicts frequently erupting in the sub-strategic domain between nuclear rivals. Cyber-security is the product of the 21st century and therefore, it is unfamiliar with the code of conduct of the previous century. Strategists are still trying to locate cyber threats as strategic or sub-strategic. For nuclear weapon states like India and Pakistan, it is a dual dilemma, both to identify the danger and to devise a strategy that does not disturb the strategic balance.

The scholarly literature revolving around the stability-instability paradox mainly relies upon the premises of conflict between mutually deterred nuclear states of South Asia, India and Pakistan. India and Pakistan developed friction even before their inception. Both states hold multipronged animosities against each other based on cultural, historical, and religious grounds. Nevertheless, at the core of the conflict are political interests, both strategic and sub-strategic. This particular research will identify cyber-friction between the two states as a conflict of sub-strategic domain. Considering the nature of the equation between the two states, the case will be identified as relevant to the red-line or brinkmanship models. It will finally evaluate the escalatory potential of the cyber equation between the two states, keeping in view their mutually deterred posture, as well as the impact of this cyber-friction on the nuclear posture of the two states. The article is divided into three parts: The first part develops the conceptual framework based on the scholarly debate over the stability-instability paradox. The second part evaluates the strategic stability-instability equation between India and Pakistan, the two arch-rivals of South Asia. The final part evaluates the Cyber-security equation and vulnerability of strategic balance between the two states.

Stability-Instability Paradox

Cold-war decades not only transformed the political world order, but the intellectual one also evolved. New inventions during the Cold War called for developing a new theoretical base in international relations and strategic studies. The concept of the stability-instability paradox is a product of the same time; it emerged as a theoretical base behind the limited confrontation between nuclear rivals. After the atomic explosion of 1945 over Japan, no major nuclear war emerged. The Cuban missile crisis was the closest that the Cold War witnessed. There were proxy wars, but the two rivals, the US and the USSR, avoided confrontation. Keeping these dynamics in view, the concept of nuclear deterrence made its space in the domain of International relations. The reason behind no major confrontation was identified as the fear of nuclear war. However, the reason behind proxy wars and minor conflicts was still ambiguous. In this realm, the concept of stability-instability paradox emerged. In 1965, Glenn Snyder proposed the idea for the first time, defining it as "Greater the stability of the greater strategic balance, lower is the stability of overall balance at lower levels of violence."[3]

The end of the Cold War rendered many intellectual debates redundant. However, the discussion on the stability-instability paradox remained unsettled. Literature involves a multitude of explanations of the concept. Kapur stated that the literature lacks consensus regarding the second aspect of the idea: instability[4]. Explanation regarding the cause behind the emergence of instability on a lower strategic level between two mutually deterred adversaries varies from scholar to scholar. Kapur has categorised these explanations into three groups. The first group questions the validity of Nuclear deterrence and claims that instability erupts at lower levels with an escalatory potential that can even lead to a full-fledged nuclear conflict. On the contrary, the second group believes that lower-level conflicts emerge without escalatory potential because of mutual nuclear deterrence. The third group barely talks about nuclear deterrence without touching the disputes that erupt at the lower strategic levels. Michael Cohen has criticised Kapur's non-escalator model, stating that it is irrelevant to the stability-instability paradox.[5]

Considering the controversy surrounding the explanation of the stability-instability paradox, this research will mainly rely upon the conceptual framework developed by Christopher. J. Watterson[6]. The proposed framework first settles the difference between strategic and sub-strategic domains and then determines that the scenario varies from case to case. In some cases, conflict at the sub-strategic level can escalate into a strategic war, while it lacks the escalatory potential in other cases.

However, the concept is not as generic as it seems; it is based on two models that explain possible scenarios: the red-line and brinkmanship models.

As Watterson proposed, war is an extension of a political bargain. Therefore, the escalatory potential of the conflict depends upon the stakes involved. States usually have two major categories of political objectives: strategic and sub-strategic. Strategic goals are those considered to be associated with the state's existence and therefore, cannot be neglected. However, sub-strategic domains are relatively less significant for the state. Watterson proposes that the escalatory potential of the conflict depends upon the extent of its strategic motive.

In the red-line model, both the parties to the conflict have a mutual agreement on the intenability of nuclear conflict and therefore, they comfortably allow conventional conflicts to escalate. The belief that nuclear war will never emerge because it is against both states' strategic objectives lies at the core of this explanation. On the contrary, the brinkmanship model explains that the fear of nuclear escalation underlines the sub-strategic conflicts. It presumes that the risk of nuclear escalation threatens both parties to the conflict. However, one of the two parties would always find a situation to exploit this fear for sub-strategic gains, hoping the other party would agree to its conditions out of the fear of nuclear escalation. Overall, this model proposes that the emergence and conclusion of any sub-strategic conflict depends upon the mutual belief of the states on the devastating impacts of nuclear conflict, the exploitative intent of one of the states and the balance of resolve between the two. In this manner, Watterson has provided a framework to evaluate the impact of nuclear deterrence on the sub-strategic conflicts between adversarial states and the effect of the sub-strategic conflicts on the atomic equation between the two.

Cyber-attacks are relatively unconventional threats; therefore, categorising them under strategic or sub-strategic categories is challenging. Thus, the paper aims to evaluate cyber-security threats' impact on the strategic balance between the mutually deterred arch-rivals.

Mutually Deterred Arch Rivals of South Asia

Tracing the history of India and Pakistan's relations reveals intricate connections, ongoing conflict and a delicate balance of power. Throughout their diplomatic history, strategic miscalculations and misperceptions have arisen due to this dyadic interaction, which has impacted the complex historical legacies of both parties. These cognitive biases play an essential role in defining the contours of this complex relationship, frequently bringing both parties to the verge of heightened

tensions, misunderstandings and even conflict. Against this backdrop, it becomes eminent to investigate the causes and underlying factors that perpetuate the same cycle of misunderstandings and misperceptions between these two neighbouring countries.

The histories of India and Pakistan are intertwined due to their shared colonial past, mutual desire for independence and the subsequent partition in 1947. The primary intent of this separation was to establish separate entities based on religious beliefs; however, it has left a legacy of confusion that has fostered mistrust and hatred. The tumultuous founding of these two nations, set against mass migrations, pervasive violence and unhealed wounds, fostered a climate in which historical grievances reverberate with permanent resonance. This tragic past has left an indelible mark not only on their bilateral interactions but also on the cognitive prism through which they interpret the motivations and actions of the other.

In this historical context, narratives have evolved into potent tools for constructing identities and forging nations. India and Pakistan have each developed narratives that extol their grandeur while highlighting the shortcomings of the other. These narratives, which are frequently meticulously fostered through education, media, and political discourse, shape citizens' perceptions of their own nation's moral standing and the alleged wrongdoings of the opponent. The disparity between these narratives creates an environment in which strategic decisions are interpreted through the lens of preconceived notions, which can have long-lasting effects on a partnership.

The unstable balance of power adds another layer of complication to the global landscape. Both nations possess nuclear weapons and are determined to use them to defend their national interests. However, in the context of the Stability-Instability Paradox, possessing atomic weapons has uniquely impacted their conflicts. While nuclear weapons introduce a level of instability due to the catastrophic potential of their use, they paradoxically create stability by deterring all-out wars. The evidence for this is obvious. India and Pakistan have had three full-scale wars beginning in 1947-48, 1965, and 1971. After both states acquired nuclear weapons, no full-scale war has taken place. The latest instance of both countries locking horns was in 2019 during the Pulwama-Balakot episode, in which Pakistan downed two Indian fighter jets after their unwarranted infiltration of Pakistan's territory[7]. However, this also did not lead to a full-scale war.

The spectre of strategic miscalculations and misperceptions haunts complex, conflicted, and delicately balanced interactions between India and Pakistan. These misunderstandings, rooted in their shared history and narratives,

create a world where positive intentions are frequently misinterpreted. These miscommunications contribute to a culture of mistrust, heighten tensions and can even bring the region to the brink of conflict.

Historical Legacy

Strategic miscalculations and misperceptions have a long and storied history in the convoluted web of Indo-Pakistani relations. In the dynamic of this couple, the weight of history has left an indelible impression on the present and will continue to do so for the foreseeable future. Notably, a substantial portion of these misconceptions can be traced back to India and Pakistan's shared historical past. The partition of 1947 will be inscribed indelibly into the collective memory of the subcontinent's inhabitants. Nationalist ideals inspired this period of liberation, which paradoxically led to the division of the sub-continent. As a result of widespread human displacement, inter-communal violence and unfathomable misery, the region's landscape and its inhabitants souls are irrevocably scarred. This turbulent environment was ideal for the growth of mutual mistrust and dread, which sprouted like weeds from the seeds of ingrained mistrust[8].

The legacy of mistrust left by the separation has distorted how the two countries view each other's actions and intentions. Emotionally charged grudges handed down through generations contribute to developing cognitive biases and cloud judgment. Unresolved territorial conflicts cast a lengthy shadow over international relations; Kashmir is a prime example of this trend. Regardless of how sincere their intentions may be, the protracted nature of these disagreements creates an environment where benevolence is viewed with suspicion, and the possibility of hidden agendas exists at all times.

In this tale of historical legacy and unresolved resentment, the psychology of Indo-Pakistani relations takes on a particular hue. The past is not just a repository of memories; it also actively influences the patterns of contemporary relationships. When memories of past betrayals and injustices merge with contemporary goals, the line between historical truths and perceived realities dissolves, making it challenging to distinguish intentions from interpretations.

The Indo-Pakistani relationship is a prominent example of how history imprints every aspect of international relations, from diplomacy and geopolitics to national pride and individual identity. Untangling the tangled web of misunderstandings and false assumptions requires active participation in the present and a fearless journey into the past. At that point, the chains of miscommunication

will unravel and a more sophisticated understanding will emerge from the shadows of the past.

National Narratives and Identity

Creating and disseminating national narratives substantially affects a population's psyche, influencing the assumptions and presumptions that drive interstate interactions. The interplay between narrative production, identity formation and strategic misunderstandings is crucial to the Indo-Pak geopolitical landscape. In this tense environment, both India and Pakistan have crafted narratives that highlight the assets of their respective countries while disparaging those of their rival. These narratives, meticulously crafted and disseminated through educational, journalistic, and political discourse channels, play a crucial role in fostering an environment where misunderstandings and incorrect assumptions about motivations are prevalent.

Each nation's narrative architecture serves as a psychological fulcrum, providing its citizens with something substantial to anchor their sense of identity, legitimacy, and desire. After decolonisation and the visceral turmoil of separation, India and Pakistan undertook nation-building initiatives characterised by a genuine desire to unite disparate identities into a unified whole. In this effort, stories served as the adhesive that binds individuals from diverse backgrounds and language groups together.

The history of India as the "Jewel in the Crown" of the British Empire is woven into a narrative that glorifies the nation's pluralism, democracy and cultural legacy. It promotes itself as a place where individuals from all aspects of life can celebrate their differences while retaining a sense of unity. While this story is based on actual events, specific details have been simplified to promote a more cohesive and admirable national identity.

On the other side of the frontier, Pakistan's history was shaped by the ideological currents underpinning the division. This narrative depicts Pakistan as a haven for a distinct religious and cultural ethos, one that has its roots in Islam and endeavours to carve out a homeland for Muslims on the Indian subcontinent. It employs past injuries and wrongdoings to defend the nation against future threats from within and without.

These stories spread like wildfire throughout the public sphere, from media pulpits to government chambers. Heroes and their courage and perseverance are celebrated, but any events that could cast a shadow on the larger narrative are

glossed over or omitted entirely. State-run and private media entities propagate and reinforce these narratives, solidifying the public's perception of a nation's relative strengths and weaknesses.

It is a conducive environment for making weak decisions. The meticulously constructed narratives cause each nation to view the actions and motivations of the other through a biased lens. Unsurprisingly, deviations from the established narratives are interpreted as deviations from the accepted norm. It is a pernicious cycle of misunderstanding and mistrust perpetuated by questioning one's narrative, which is inconsistent with the established identity.

Such misunderstandings foster an environment in which exaggerated fears of peril and suspicions of hidden agendas are not only possible but almost inevitable. When contrasted with the other country's alleged flaws, one's country's advantages appear even more prominent. As a result, strategic movements are often misinterpreted as offensive rather than defensive, sowing the seeds of unintended escalation.

In the complex environment of Indo-Pakistani relations, misunderstandings based on shared narratives continue to be a significant obstacle. As long as the tales are believed, coexistence will remain unattainable. The first step is to comprehend how these narratives influence our perspectives to untangle the web of strategic misunderstandings that have grown to penetrate this tense relationship.

Security Dilemma

In the Indo-Pakistani context, the security dilemma is a complex and potent force that perpetually drives strategic dynamics toward unforeseeable outcomes. The anarchic character of international relations necessitates the existence of this conceptual framework, which serves as a crucible in which the security measures adopted by one state pose a threat to another. The acquisition of nuclear weapons by both India and Pakistan has added a distinct layer of complexity to this security dilemma. The nuclear foundations of both nations raise the stakes and amplify the risk of error, thereby making the core of this issue more precarious[9].

India and Pakistan are both nuclear powers; consequently, they must maintain a balance that enables them to safeguard their national security. Each party takes precautions to ensure its survival, but these actions paradoxically set off a domino effect that sows the seeds of mistrust and escalation. The most apparent manifestation of an arms race is a build-up of military forces, which functions as both a deterrent and a warning signal. Even though the stated purpose of the

weapons is to deter conventional attacks, the Stability Instability Paradox comes into play; Pakistan's development of tactical nuclear weapons has become entangled in a web of misperceptions, evoking fears of possible battlefield use that resonate across the border[10].

When viewed from the opposing side, these defensive measures appear aggressive. This contradiction lies at the core of the security dilemma. As actions and reactions become entangled in a web of misinterpretation and mistrust, the security issue transcends borders and cultures. This pernicious cycle of mistrust only exacerbates the already tense Indo-Pakistani relationship and ensures that strategic errors will continue to be made. The perception of provocation clouds the judgment of both parties, and the haze of uncertainty obscures the motivations for defensive actions. In this context, the security dilemma is a double-edged sword, aggravating existing tensions and making conflict resolution and cooperation more difficult.

The security dilemma plays a particularly crucial role in the context of the troubled history and profoundly ingrained narratives that have shaped Indo-Pakistani relations. Introducing cyber warfare as a potential avenue is an illustrative manifestation of the Stability-Instability Paradox. For this situation to persist within the nuclear dimensions of the region, a comprehensive understanding of the interplay between actions, perceptions, and strategic outcomes is required.

The Cyber Equation between Pakistan and India: Threats and Vulnerabilities

Over the period, Indo-Pak animosity has displayed the potential to increase in magnitude and lethality due to the invention of novel technologies. The nuclearisation of South Asia was one such instance that changed the direction, augmented the lethality of the rivalry and demanded responsible behaviour from the neighbouring states. Nuclear weapons are still the most destructive weapons that both powers possess. However, new instruments and avenues of warfare have emerged whose strength, unlike nuclear weapons, lies not in their presence as deterrents but in their actual use. Also, cyber security has become a prerequisite for nuclear security.

There have been instances where states have utilised cyber technology to attack the nuclear infrastructure of other states. Israel's Operation Orchard, in this regard, is one prominent instance where it used cyberspace to dismantle Syria's purported nuclear reactor successfully. Also, the Stuxnet attack on Iran carried out simply through USB keys, shows that even air-gapped networks are unsafe from

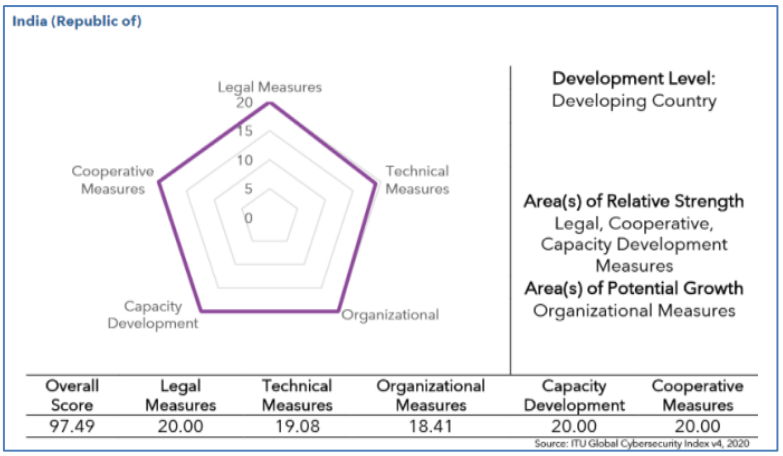
cyber-attacks, and their vulnerability will only increase.[11] There is every chance that in the future, cyberspace may more frequently be used to target nuclear capabilities.

Cyber weapons are also problematic because, unlike nuclear weapons, their use does not carry as much potential to lead towards absolute war or MAD. Numerous militaries across the globe have cyber warfare doctrines, and cyber warfare units are also being established to improve cyber security readiness. Although no Offensive Cyber Operation has resulted in a traditional war to date, there is potential that such attacks can be protracted.[12]

Cyber Capabilities of India and Pakistan

India and Pakistan are both on the path to development in the field of cybersecurity. The International Telecommunication Union (ITU) is a UN-specialized agency that evaluates and ranks certain states' progress in the cyber-security domain. The agency's evaluation criteria encompass five essential elements: legal, technical, organisational, capacity building, and international cooperation. The report categorises states into three categories: leading, maturing, and initiating. According to the 4th edition of the report, Pakistan has scored 64.88 and ranked 79/183 in the Global Cybersecurity Index[13]. It is on the maturing or developmental level, as shown in Figure 1. The country, however, has focused more on legal development and lacks progress in countering cyber-attacks, especially when it faces a grave threat from the rapid increase in India's cyber capabilities.[14]

Figure 1: Pakistan's profile on the Global Security Index 2020

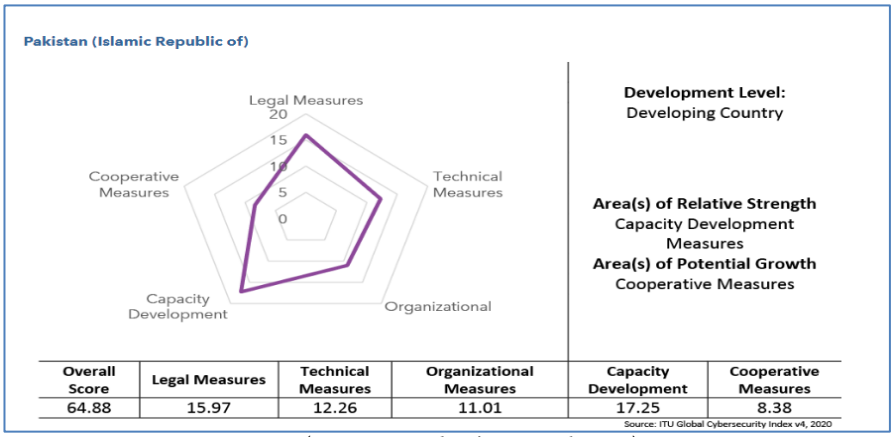


(Source: Author's compilation)

India, on the other hand, ranks 10/183 with a score of 97.5. Its status has rapidly improved, and its capabilities concern all the regional states. It has developed strength in the areas of the legal and cooperative side of capacity development

measures. However, it is necessary to focus more on organisational measures, as demonstrated in Figure 2.

Figure 2: India's Profile on the Global Cyber-Security Index



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
64.88	15.97	12.26	11.01	17.25	8.38

Source: ITU Global Cybersecurity Index v4, 2020

(Source: Author's compilation)

In the context of the existing security dilemma between the two states, an increase in capabilities also leads towards an increase in vulnerability and the threat of escalation, respectively. With these developments in place, the strategic landscape between India and Pakistan has changed, with an increase in cyber-confrontations.

Role of Cyberspace in the South-Asian Context

In this age of Information and Communication Technology (ICT), Cyberspace has become another field of competition for states across the globe. States are also more prone to using cyber tools against adversaries because they enable them to 'subdue the opponent' even 'without fighting'.[15] For instance, numerous hackers from India and Pakistan have hacked and defaced essential databases. 1998, Pakistani hackers hacked the Indian Bhabha Atomic Research Center's website. Also, in 2008, Indian hackers defaced several Pakistani websites after the Mumbai attacks.[16]

In this age of digitalisation, it has become evident that ICT has become an essential tool in everyday life. From domestic affairs such as utility billings, industry, finance, and health to foreign relations and ensuring the security of states, everything is linked with ICT in some way. Cyber Readiness is. Thus, states entangled in conflict must consider this and continue to build upon it. States like Pakistan can take steps towards cyber readiness by utilising the UN International Telecommunication Union's prescribed five pillar criteria: international, technical, organisational, capacity building and legal cooperation.[17] Cyber capabilities are also crucial because they have become a source of prestige for states. Cyber power is

undoubtedly an instrument that will continue to play a vital role in the future survival of states.

Cyberspace is famous for its utility in informing and educating the masses across the globe about the latest news and trends. However, the same also carries the potential to be misused to promote an anti-state narrative by both hawkish terrorist groups and hostile states to destabilise rivals. This has brought humanity to the new age of cyber warfare and hybrid warfare, where, besides conventional aggression, mutually hostile actors remain busy sabotaging rival states' digital capacity.[18]

Table 1: Cyber-Attacks by India and Pakistan (1998-2017)[19]

Date	Event
05.1998	Pakistani hackers have hacked the Indian Bhabha Atomic Research Center's website (Garsein, 2012).
10.1999	Pakistani hackers deface an Indian Army propaganda website with messages denouncing torture in Kashmir by the Indian Army (BBC News, 1998).
23.10.2001	Pakistani patriotic hackers deface two Indian news websites (Majumder, 2001).
28.11.2008	As retaliation for the defacements, Pakistani hackers deface Indians. websites (RFSID, 2016; Ribeiro, 2008).
01.2010	Pakistani and Indian troops exchange fire in Kashmir across the Line of Control (Hashim, 2014).
03.12.2010	Pakistani hackers hacked and erased data on the Indian Central Bureau of Investigation website as retaliation for the defacements of November 2010 (Leyden, 2010).
29.11.2011	Indian hackers deface hundreds of Pakistani websites (Kumar, 2011a).
12.2011	A series of tit-for-tat cyberattacks occur between Indian and Pakistani hackers until February 2012 (Joshi, 2012).
26.01.2012	Independently from the series of cyberattacks mentioned above, Pakistani hackers defaced more than 400 Indian websites on the Indian Republic Day (Mid Day, 2012).
15.08.2012	Indian Hackers deface Pakistani websites on Pakistan Independence Day (Garsein, 2012).
17.03.2013	A Norwegian telecommunications firm reveals that it has been targeted by a cyberespionage campaign that is possibly coming from India. (Fagerland et al., 2013).

26.11.2013	Indian hackers deface several Pakistani websites on the anniversary of the Mumbai terrorist attacks. Pakistan Cyber Army, a Pakistani patriotic hacker group, retaliates by defacing the website of the Indian. Central Bank (Kovacs, 2013a).
26.01.2014	Pakistani hackers deface thousands of Indian websites on the Indian Republic Day (Khan, 2014).
26.11.2014	Indian hackers deface several Pakistani government websites on the anniversary of the Mumbai terrorist attacks (Web Desk, 2014).
07.01.2016	Indian hackers retaliate for the terrorist attack in Pathankot with the defacement of Pakistani websites. (RFSID, 2016).
03.03.2016	Pakistani authorities arrested an Indian individual suspected of espionage in Pakistan (Shukla, 2017).
15.08.2016	Indian hackers deface more than 50 Pakistani websites on Pakistan Independence Day (TNM Staff, 2016).
10.04.2017	Indian hackers retaliate with the defacement of hundreds of Pakistani websites to protest against their compatriot's death penalty sentence. (Trivedi, 2016).

Warfare has transformed, and besides kinetic attacks, cyberspace has emerged as another deadly tool to cause multi-dimensional damage to rivals by using the digital front. Also, cyber-attacks are a more cost-effective and potent approach to damage an enemy than conventional physical attacks.[20] Usually, states use cyber technology to carry out offensive operations (commonly known as Offensive Cyber Operations) at two different levels, which include Computer Network Attacks (attacks on adversary's computers for destroying, gathering data, etc.) and Cyber-physical attacks that target installations with larger physical setups such as transportation, financial systems, power and electricity sectors, etc.[21] In the Indo-Pak context, frequent Cyber-attacks on one another can swiftly lead to escalation and, thus, damage regional and international stability. Pakistani side already considers cyber/fifth generation warfare (5GW) a grave threat, and there are increasing discussions in policy-making circles about avoiding cyber threats and complexities. Even besides state-to-state interactions, cyberspace carries multiple challenges. For instance, it is also used by terrorist organisations for recruitment purposes, psychological warfare and as a means to communicate with targeted masses to generate support.[22] Cyber security is. Thus, it is a domain in which states across the globe are establishing their expertise to tackle any threat to national security.

Pakistan's Cyber Security Challenges and the India Factor

Pakistan ranks 10th most significant in terms of the number of internet users worldwide. However, the fact that, in 2017, Pakistan ranked 67th out of 193 countries in the Global Cyber Security Index's (GCI) annual report shows that the country is vulnerable to cyber threats. Pakistan's decision-making bodies, such as the senate's standing committee, are well aware of the country's readiness challenges to counter cyber threats.[23] Simultaneously, India already recognises information warfare (which includes cyber warfare and attacks on enemy computer systems) as a component of its Cold Start doctrine. In 2016-17, India also concluded 17 agreements with different states, including the UK, the US, Israel, France, etc., to gather assistance in further developing its cybersecurity infrastructures.[24]

Meanwhile, Pakistan has already experienced the application of India's cyber warfare strategy on numerous occasions. In 2018, the cellular devices of senior Pakistani officials were hacked, purportedly, by India through a software called 'Pegasus' which is used for illegal surveillance purposes. Later on, it was observed that the same had been utilised by the Indian intelligence for domestic surveillance, as well.[25] India has been involved in cyber-attacks on Pakistan for a long, and according to some sources, between 1999 and 2008, as many as 1600 Pakistani websites were attacked by Indian hackers. The Indian side focuses more on cyber capacity building through novel ideas such as creating the Indian Cyber Army (ICA) comprising professionals with expertise who successfully hacked the websites of Pakistan's essential government institutions, including NADRA, NAB, MOFA, etc.[26] To counter such incursions in the future, Pakistan also needs to follow suit and develop a more inclusive approach to tackle cybersecurity-related issues.

Due to the prolonged animosity, both the states have always seen each other as a serious threat to their internal stability and prosperity. During the previous government, then Pakistan's Foreign Minister Shah Mehmood Qureshi claimed on mainstream media that the government has substantial evidence of Indian involvement in supporting terrorist groups, including BLA, Jamaat-ul-Ahraar, etc., in Pakistan.

Disinformation and propaganda are also significant tools utilised to infuriate the grievances of people from underdeveloped areas and communities. India has constantly depended on cyber, proxy, and information warfare to target Pakistan's national security, which needs to up its cyber defensive wherewithal, which, according to Comparitech's recent findings, is the seventh worst cyber security country.[27] Cyber-attacks, in the past, on public and private bodies, including FBR and K-electric, are evidence of Pakistan's vulnerability in front of cyber

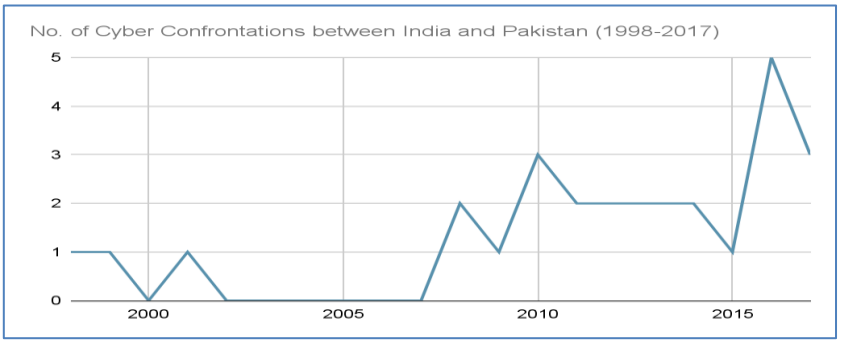
criminals who demand hefty payments. To make things worse, envious states and terrorist organisations can also utilise these terrorist factions for hawkish gains.[28]

Cyber-Security and Strategic Imbalance: From Red-Line to Brinkmanship

Seventy-six years of animosity between India and Pakistan have impacted mainly the strategic balance in South Asia. Ever since the inception of nuclear rivalry, the strategic balance has been standing upon the mutual belief in the tenability of nuclear conflict. Both states have been confronting each other on various fronts, believing that minor sub-strategic conflicts would never escalate into a full-blown nuclear conflict, as it will cost more than they can afford. Therefore, an outbreak of strategic conflict, let alone a nuclear conflict, has been a red line for both states. Outbreak of the conflicts in the sub-strategic domains has depended on the respective capabilities of states in those domains.

The nature of conflict, nevertheless, has evolved over the years. Developments in the cybersecurity domain have blurred the distinctive line between the strategic and the sub-strategic, making the strategic parameters and models irrelevant. The ambiguity involved in cyber operations that do not unveil the perpetrators and their objectives has complicated the matters of strategic calculations. Furthermore, the scope of the strategic vulnerability of states in the wake of cyber-attacks must be revisited. Cyber-attacks can either be launched over any state's direct military facilities or security apparatus or indirectly by sabotaging the power facilities or hacking private accounts of the workforce that can compromise the state's security. Therefore, Cyber-security has made it ambiguous for the states to determine a) Whether the attack was strategic or sub-strategic, b) What the plan of action to retaliate against it (Offensive/defensive), c) The possibility of nuclear escalation, as a result of this attack.

Graph-1: No of Cyber Confrontations between India and Pakistan over the Years



(Source: Author's compilation)

In the given case of Indo-Pak rivalry, a historical overview has determined the persisting discord that has penetrated generational perceptual build-up and will require generations to be uprooted. However, a chronology of events in Cybersecurity indicates that both states are gradually moving from the red-line model to the brinkmanship model. Frequent episodes of cyber-attacks and counter-attacks from both sides indicate that one of the two states has been less considerate of the overall impact of escalation and more mindful of the vulnerability of the other state. Indian aspiration of regional hegemony has always faced significant resistance from the next-door nuclear power. However, through the past decade, India has shown a rather assertive posture in mutual strategic calculation. For instance, the abrogation of the article-370 of its constitution to alter the status of IIOJK indicated the motives of brinkmanship from the Indian side.

Therefore, the equation moves towards a balance of resolve and Cybersecurity makes the equation even more sensitive. If India keeps on considering the escalation of nuclear conflict as a vulnerability of Pakistan and keeps on taking assertive actions, it will push Pakistan to take action. With the cyber infrastructure in place, both states can indirectly get entangled in a spiral of conflict. This, however, cannot only disturb the overall strategic balance but is also likely to lead towards a full-blown nuclear escalation if measures are not taken to establish a code of conduct in the cyber domain.

Future Strategies for India and Pakistan to Avoid Cyber Conflict Protraction

There are several ways in which Pakistan and India can cooperate to avoid the protraction of conflicts emerging from cyberspace, such as creating a joint committee with experts from both sides to probe and mitigate crises. Other ways to avoid cyber conflicts include creating hotlines similar to the existing DGMO hotline and devising an apparatus that could be fruitful in avoiding attacks on critical infrastructure. These confidence-building measures can be a source of relief for the international community and help promote the image of both countries as responsible international stakeholders.[29]

Moreover, the hawks would never cease to exist, and thus, along with CBMs and other cooperative measures, states must constantly prepare themselves to tackle potential cyber threats and attacks. Defensive approaches to protect systems from unwanted breaches are needful. Defense Cyber Operations Response Actions (DCO-RA) are measures to protect computers through malware and botnet scans, creating DNS servers, authentication, etc. In this way, DCO-RA functions just as the immune system functions in the human body. Simultaneously, passive Defence mechanisms

protect systems from the outside and pre-empt incursions. Cyber deterrence is also one thing that can help states avoid attacks. For instance, During Donald Trump's term as President, his security advisers displayed reluctance in attacking North Korea because they feared North Korea's cyber retaliation.[30]

The cyber domain has increased friction, uncertainty and mistrust between South Asian neighbours, but it still has the potential to become a field of collaboration. Pakistan and India have cyber security concerns and with constructive intent, these concerns can also be translated into shared cyber security goals. Given the state of the bilateral relationship, it seems that collaboration may not be possible shortly. However, simple steps such as adopting and abiding by the principles and healthy practices can make the situation much more accessible for Pakistan and India in an international order where cyberspace will continue to increase.

Conclusion

Seventy-six years of animosity between India and Pakistan have shaped the strategic balance between the two states. Ever since the inception of nuclear rivalry, the strategic balance has been standing upon the mutual belief in the tenability of nuclear conflict. Both states have been confronting each other on various fronts, believing that minor sub-strategic conflicts would never escalate into a full-blown nuclear conflict, as it will cost more than they can afford. Progression of Cybersecurity threats, however, has complicated the equation. The red-line model South Asia's nuclear arch-rivals have been following is likely to be replaced by the brinkmanship model, provided the strategic discombobulation associated with cyber-security prevails. Research has found an increase in the number of cyber-attacks and counter-attacks between India and Pakistan, with an overall disturbance of the strategic balance. The hegemonic aspirations of India and the uncompromising defensive posture of Pakistan can pave the way for the rupture of cyber-brinkmanship into a nuclear escalation. Therefore, both states should acknowledge the need to establish cyber-security regimes and take precautionary measures to spare the future from the shadow of unseen wars.

References

[1] "Cybersecurity Breach at NIFT Puts National Security at Risk," The Express Tribune, June 22, 2023, https://tribune.com.pk/story/2423250/cybersecurity-breach-at-nift-puts-national-security-at-risk.

[2] Diakun-Thibault, Nadia. "Defining Cybersecurity." *Technology Innovation Management Review*. October 31, 2014.

[3] Snyder, Glenn. "The Balance of Power and the Balance of Terror" In The Balance of Power, edited by Paul Seabury,184-201. San Francisco: Chandler, 1965.

[4] Kapur, S. Paul. Dangerous Deterrent: Nuclear Weapons Proliferation and Conflict in South Asia. Stanford, CA: Stanford University Press, 2007.

[5] Cohen, Michael D. "How Nuclear South Asia Is Like Cold War Europe," Nonproliferation Review 20, No. 3 (2013): 33–51

[6] Watterson ,Christopher J." Competing interpretations of the stability–instability paradox: The case of the Kargil War." The Nonproliferation Review. DOI: 10.1080/10736700.2017.1366623,2017.

[7] Hashim,Asad. "Pakistan Shoots down Two Indian Fighter Jets: Military."Al Jazeera. Accessed August 13, 2023. https://www.aljazeera.com/news/2019/2/27/pakistan-shoots-down-two-indian-fighter-jets-military.

[8] "India-Pakistan Partition 1947," accessed August 12, 2023. https://www.globalsecurity.org/military/world/war/indo-pak-partition.htm.

[9] Gilgrist,James. "The 'Security Dilemma' and South Asian Nuclear Relations: India-Pakistan," *E-International Relations*. January 22, 2008. https://www.e-ir.info/2008/01/22/the-'security-dilemma'-and-south-asian-nuclear-relations-india-pakistan/.

[10] Ahmed, Mansoor. "Pakistan's Tactical Nuclear Weapons and Their Impact on Stability." Carnegie Endowment for International Peace. Accessed August 12, 2023. https://carnegieendowment.org/2016/06/30/pakistan-s-tactical-nuclear-weapons-and-their-impact-on-stability-pub-63911.

[11] Ashraf, Ms Nageen and Dr Saima Ashraf Kayani. "INDIA'S CYBER WARFARE CAPABILITIES: REPERCUSSIONS FOR PAKISTAN'S NATIONAL SECURITY." *NDU Journal* 37 (May 23, 2023): 38. https://doi.org/10.54690/ndujournal.37.152.

[12] Leuprecht,Christian, Joseph Szeman, and David B. Skillicorn."The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity." *Contemporary Security Policy* 40, no. 3 (July 3, 2019): 392. https://doi.org/10.1080/13523260.2019.1590960.

[13] "ITU Publications." Accessed December 16, 2023. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

[14] Shad,Muhammad Riaz. "Cyber Threat Landscape and Readiness Challenge of Pakistan." *Strategic Studies* 39, no. 1 (April 24, 2019): 15. https://doi.org/10.53532/ss.039.01.00115.

[15] Gichki,Aqeel Ahmad."The Role of Media in the Fifth Generation Warfare: The Indian Information War against Pakistan." *Journal of Mass Communication Department, Dept of Mass Communication, University of Karachi* 27 (December 31, 2022): 51, http://www.jmcd-uok.com/index.php/jmcd/article/view/240.

[16] Baezner, Marie. "Regional Rivalry between India-Pakistan: Tit-for-Tat in Cyberspace." *CSS Cyberdefense Hotspot Analyses*. ETH Zurich, August 2018. https://doi.org/10.3929/ethz-b-000314582.

[17] Shad,Muhammad Riaz. "Cyber Threat Landscape and Readiness Challenge of Pakistan." *Strategic Studies* 39, no. 1 (April 24, 2019): 15. https://doi.org/10.53532/ss.039.01.00115.

[18] Khan,Muhammad Imad Ayub. "CYBER-WARFARE: IMPLICATIONS FOR THE NATIONAL SECURITY OF PAKISTAN." 2019., 101.

[19] "Hotspot Analysis: Regional Rivalry between India- Pakistan: Tit-For-Tat in Cyberspace." CSS CYBER DEFENSE PROJECT, 2018. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf.

[20] Ashraf ,MS Nageen,and Dr Saima Ashraf Kayani. "INDIA'S CYBER WARFARE CAPABILITIES :REPERCUSSIONS FOR PAKISTAN NATIONAL SECURITY." NDU Journal 37 (2023):37.

[21] Leuprecht, Szeman, and Skillicorn. "The Damoclean Sword of Offensive Cyber :Policy Uncertainity and Collective Insecurity ." Page 387.

[22] Khan,Muhammad Imad Ayub. "CYBER-WARFARE: IMPLICATIONS FOR THE NATIONAL SECURITY OF PAKISTAN." 2019., 101.

[23] Shad,Muhammad Riaz. "Cyber Threat Landscape and Readiness Challenge of Pakistan." *Strategic Studies* 39, no. 1 (April 24, 2019): 15. https://doi.org/10.53532/ss.039.01.00115.

[24] Ibid.

[25] Khan, Umair Pervez and Muhammad Waqar Anwar. "CYBERSECURITY IN PAKISTAN: REGULATIONS, GAPS AND A WAY FORWARD." 2020, 208.

[26] Shad,Muhammad Riaz. "Cyber Threat Landscape and Readiness Challenge of Pakistan." Page 9.

[27] Gichki,Aqeel Ahmad."The Role of Media in the Fifth Generation Warfare: The Indian Information War against Pakistan." *Journal of Mass Communication Department, Dept of Mass Communication, University of Karachi* 27 (December 31, 2022): 51, http://www.jmcd-uok.com/index.php/jmcd/article/view/240.

[28] Ashraf and Kayani, "INDIA'S CYBER WARFARE CAPABILITIES," 37.

[29] Khan,Abdul Moiz. "Cyber Deterrence and Confidence Building Between Pakistan and India." South Asian Voices, February 2, 2023. https://southasianvoices.org/cyber-deterrence-and-confidence-building-between-pakistan-and-india/.

[30] Leuprecht, Christian,Joseph Szeman, and David B.Skillicorn. "The Damoclean Sword of Offensive Cyber:policy Uncertainity and Collective Insecurity." Page 392.