NUML-Journal of Research in Social Sciences (JRSS)
Vol No 12, No 01, January 2024. pp 25-47

ISSN: 2306-112X (E); 2305-6533 (P)
https://doi.org/10.52015/jrss.12i1.235

Pakistan in the Crosshairs and the Rising Stakes of Strategic Information Warfare

Sahibzada Muhammad Usman[1]

Article History:

Received:
October 16, 2023
Accepted:
December 05, 2023
Published:
January 11, 2024

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Abstract:

Over the past two decades, information and communication technologies (ICTs) have reaped significant attention from security experts, computer scientists, intelligence agencies, and governments for their potential applications in conflict scenarios. Using ICTs for offensive or defensive purposes to instantly invade, disrupt, or control the opponent's resources is known as strategic information warfare (SIW). Although SIW is as ancient as military history, the communication sciences revolution has altered its character. It has evolved into a double-edged weapon that is equally crucial for strong nations, technically underdeveloped states, non-state entities, and individual software experts. Some nations, most notably the US, Russia, and China, have taken the SIW technology seriously and compared it to the danger posed by WMDs. In the south Asian context, Pakistan faces a direct threat from India, which collaborates closely with Israel, by the use of SIW. Additionally, the Western media portrays a highly negative picture of Pakistan's administration, law and order, and economy. The national media, suitably supported by foreign players, has begun a propaganda warfare effort against Pakistan's military forces and intelligence institutions. However, SIW is now a global danger, necessitating a worldwide response. Pakistan must create a proactive national strategy to prepare for the problems erupted from SIW strike on the communication network, which is crucial for the operation of its nuclear facilities.

Keywords: Pakistan, Information Warfare, National Security, Cyberattacks and Propaganda.

[1] Postdoc Fellow at School of Culture and Communication, Shandong University, Weihi China. usmangull36@gmail.com

Introduction

Strategic information warfare refers to the use of information and communication technologies to manipulate or influence the perception, beliefs, and behaviors of individuals, groups, or nations for strategic purposes. It encompasses various activities such as propaganda, disinformation campaigns, cyberattacks, psychological operations, and social media manipulation. Understanding the background of strategic information warfare and its impact on Pakistan's national security requires an examination of Pakistan's national security policy, its challenges, and the complex dynamics in the region (Antoine, 2022).

Pakistan's national security policy has been a subject of analysis and scrutiny in recent years. The country's first national security policy, released in 2022, has raised concerns due to its perceived shortcomings (Ganguly, 2022). The proposal under consideration disregards the adverse consequences of its detractors on the China-Pakistan Economic Corridor. The aforementioned omission demonstrates a lack of attention to inherent vulnerabilities and a failure to address pressing security concerns effectively.

In the context of strategic information warfare, Pakistan's national security faces many threats surpassing conventional militancy's scope. The nation grapples with the multifaceted challenges of terrorism, extremism, socio-economic issues, political transformations, and regional conflicts. The security picture is further influenced by geopolitical realities, historical animosity towards Afghanistan, and Pakistan's regional ambitions. The Kashmir issue is essential to Pakistan's security discourse, influencing views and diplomatic ties with other nations (Farooq, 2021). It is essential to approach this issue with sensitivity to facilitate meaningful involvement.

The impact of strategic information warfare on Pakistan's national security is substantial. In the contemporary age characterized by the proliferation of sophisticated information technology and interconnection, manipulating and disseminating information can influence public sentiment, mold narratives, and disrupt societal stability. Like other nations, Pakistan is vulnerable to misinformation campaigns, cyberattacks, and manipulation of social media, all of which threaten its security and stability. These strategies, utilized by governmental and non-governmental entities, capitalize on pre-existing societal differences, intensify religious and ethnic conflicts, and cultivate community fragmentation.

In order to ensure the preservation of national security, Pakistan must implement comprehensive strategies that effectively tackle several interconnected variables concurrently. This involves mitigating strategic information warfare by reinforcing cybersecurity measures, the cultivation of media literacy and critical thinking, and establishing robust institutions capable of effectively fighting misinformation and propaganda. In addition, promoting international cooperation and establishing regional alliances significantly reduces the effects of strategic information warfare and enhances Pakistan's security perception (Alisha, 2020). The primary aim of this study is to examine the ramifications of strategic information warfare on Pakistan's national security, as well as to analyze the requisite methods and policies for effectively mitigating its effects.

In essence, the phenomenon of strategic information warfare poses significant difficulties to the national security of Pakistan (Zafar, 2020). Formulating the nation's national security strategy necessitates considering and resolving critical concerns, including but not limited to fiscal stability, sectarianism, and regional conflicts. Furthermore, Pakistan must recognize the intricacies of its security environment, evaluate the ramifications of strategic information warfare, and develop all-encompassing approaches to combat misinformation, cyber threats, and manipulation on social media platforms. To protect the country from this ever evolving peril of SIW, the proactive approach of Pakistan is needed to safeguard its sovereignty and integrity.

Research Question

How is strategic information warfare a threat to Pakistan's national security, and what measures might be taken to combat these dangers successfully?

Significance of study

1. Strategic information warfare constantly evolves, propelled by ongoing technological, cyberspace, and communication network breakthroughs. In formulating successful defense policies, it is crucial to acknowledge Pakistan's national security implications.
2. The susceptibility of information systems presents a concrete threat to Pakistan's economic and military security. Conducting a thorough examination of the effects of strategic information warfare is essential for recognizing possible threats and formulating suitable remedies.
3. Strategic information warfare can influence public sentiment, intensify religious and ethnic conflicts, and cultivate societal divides. Exploring the ramifications of misinformation and

propaganda on Pakistan's national security enables the development of strategic measures to address these challenges effectively.

4. A comprehensive analysis of Pakistan's difficulties and weaknesses in strategic information warfare provides a foundation for identifying areas that require enhancement in cybersecurity, media literacy, and institutional resilience.

Literature-Review

Strategic Information Warfare refers to the deliberate and systematic use of information and communication technologies (ICTs) in a strategic manner to attain a competitive advantage over enemies. The aforementioned actions are undertaken with the primary objective of attaining military, political, or economic objectives. The strategies encompass the use of various techniques to influence and exploit information and communication platforms to persuade specific target groups, construct narratives, and impede the decision-making procedures of adversaries (John, 2022). The scope of Strategic Information Warfare encompasses a wide range of tactics and strategies employed to achieve strategic objectives. One of the strategies employed in warfare is the deliberate targeting and disruption of an adversary's communication infrastructure. This may entail actions such as the disabling or jamming of communication networks. Additionally, it encompasses offensive actions directed at the adversary's information systems. This may involve the incapacitation of logistical networks or the disruption of vital infrastructure, aiming to induce operational instability and diminish their capacities.

Strategic Information Warfare is a method that utilizes cyber capabilities in order to achieve a position of information supremacy. The objective above is attained by strategically using vulnerabilities inside the adversary's networks, impeding their capacity to gather and distribute information. Psychological operations, a strategic tool in warfare, are designed to exert influence over specific target populations' attitudes, beliefs, and behaviors via the utilization of propaganda, deception, and manipulation techniques. These operations have significant importance within this particular form of warfare.

The continuous advancement of the information revolution, driven by advancements in cyberspace and information technology, has resulted in the emergence of military applications using the global information infrastructure. Therefore, the concept of information warfare has transformed to encompass a wide range of non-kinetic types of human conflict. The aforementioned elements encompass disinformation, propaganda, deceptive tactics, electronic warfare, and cyber warfare

(Robert, 2017). The onset of the First World War brought about a significant paradigm shift in combat, witnessing the convergence of many technologies and strategies. Similarly, the information age era presents many novel difficulties and prospects within information warfare. The extensive use of information technology (IT) and the Internet of Things (IoT) has resulted in the emergence of opportunities as well as vulnerabilities. Hence, organizations need to modify and cultivate proficient information warfare skills (William, 2017).

Information warfare has been seen throughout history and is not a recent development. During the First World War, the utilization of electronic warfare was observed, but the prevalence of deception operations became apparent in the Second World War (Nick, 2018). These historical examples demonstrate how the manipulation of the information environment may be utilized to exert influence over decision-making processes and achieve strategic goals. Recent wars, such as the Gulf War and the disputes between Russia and Ukraine, have underscored the significance of media operations in attaining military goals and shaping public perceptions.

The 20th and 21st centuries have witnessed a significant transformation in information warfare, mostly due to advancements in mass communications, marketing strategies, and worldwide news reporting. In summary, strategic information warfare has developed in tandem with technological progress and evolving combat environments, including various tactics and strategies. The focus of this concept revolves around obtaining a competitive advantage by strategically manipulating information and communication channels.

Strategic Information Warfare is supported by a range of theoretical frameworks that provide diverse viewpoints and methodologies for comprehending the intricate dynamics of information warfare. This discourse will examine significant perspectives derived from seminal theoretical works about strategic information warfare. The research titled "Information Warfare and the Changing Face of War" by RAND offers a significant perspective on the dynamic nature of information warfare, which is influenced by continuous improvements in cyberspace and information technology (Molander, 1996). One of the significant publications from RAND is "Strategic Information Warfare Rising," which explores the interconnectedness between the rapid expansion of the information revolution and strategic warfare. The research highlights the inherent susceptibility of information systems and recommends implementing comprehensive plans and policies to address the difficulties arising from strategic information warfare (Molander, 1998).

The scholarly article "Defining Cyberwar: Towards a Definitional Framework" proposes a comprehensive framework to establish a precise definition for cyberwarfare. This article examines the lack of a clear definition surrounding the term and highlights common elements in existing scholarly works. The text also analyzes many opinions about cyberwar, which are classified as alarmist, sceptic, and realist (Cameran, 2021).

The workshop, entitled "Rethinking Information and Cyber Warfare: Global Perspectives and Strategic Insights," brought together a panel of esteemed academics to engage in scholarly discussions surrounding theoretical aspects of cyber warfare. (RSIS, 2014). The study also delved into the political and legal dimensions of information operations and presented case studies that examine the varying perspectives and strategic approaches of different governments towards cyber warfare. The analysis emphasized the importance of developing a comprehensive comprehension of cyber warfare, given scholars' varied viewpoints and approaches in addressing cyber threats and conflicts.

The significance of information warfare is prominently emphasized within Pakistan's National Security Policy (NSP) from 2022 to 2026. The strategy significantly emphasizes strategic stability, acknowledging its pivotal significance, and encompasses several domains, including land, air, sea, cyber, and space. This statement highlights the need to strengthen cybersecurity endeavors to combat hybrid warfare and protect vital infrastructure effectively. The strategy further supports the promotion of indigenous defense manufacturing and the modernization of armed forces to address various challenges, notably those presented by India (Rabia, 2022). It fosters transparency and inclusivity in national security discussions. However, there are concerns regarding the lack of comprehensive measures in the policy to combat disinformation and protect online freedoms. It is important to strike a balance between security considerations and safeguarding free speech in the digital realm (Zaki, 2022).

Pakistan faces emerging threats in the realm of cyber warfare due to its underdeveloped cyber security infrastructure. The country's legislation remains vague and inadequate to address dynamic cyber threats. Pakistan's dependence on external technology and its ranking as one of the most targeted countries by cyber security firms further amplify its vulnerabilities. Developing a robust cyber war apparatus, focusing on prevention and establishing a national cyber policy, is crucial for protecting critical infrastructure and addressing cyber threats (Basma, 2022).

Pakistan confronts various security challenges both externally and internally. Externally, factors such as the situation in Afghanistan, evolving global power dynamics, and geopolitical changes impact regional stability. Additionally, technological advancements introduce cyber security risks. Internally, challenges include extremism, political polarization, and contest over resources. Pakistan can address these challenges through proactive foreign policy, fostering diversity, combating extremism, equitable resource distribution, and investing in education (Shoaib, 2022).

It is important for Pakistan to continue developing its cyber security capabilities, establish robust legislative frameworks, and address both external and internal security challenges to safeguard its national security in the era of information warfare.

Literature Gap

There is a dearth of in-depth examination of related cyber threats and misinformation efforts in the context of more general warfare in the literature on "Strategic Information Warfare and Its Impact on Pakistan's National Security". The amount of research on Pakistan's existing defenses against information warfare's robustness and efficacy is minimal. There is also a lack of future predictive research on dangers from growing digital warfare. Future study in these areas offers significant chances to improve our comprehension of this subject.

Research Methodology

The qualitative research approach was applied in this study. I gathered secondary data from libraries, official records, books, policy analyses, media products, websites, magazines, and peer-reviewed academic studies. By identifying underlying themes, the content analysis approach is used to analyze data and examine theoretical difficulties to better comprehend the data. Data collecting and analysis are generated via an iterative process in the case study technique because it enables the development of ideas based on actual data. I integrated these methods of investigation into the case study.

Theoretical

The theme of "Strategic Information Warfare and Its Impact on Pakistan's National Security" lends itself to a conscientious examination of how information warfare affects Pakistan's national security environment using the constructivist theory. The relevance of rules, concepts, and identity constructs is emphasized by constructivism. It can help us comprehend how perceptions and identities of state and non-state actors, both within and outside Pakistan, impact their actions and reactions in the context of information warfare.

For instance, Pakistan's policy choices surrounding information warfare may be significantly influenced by how it views its identity in the global digital ecosystem (as a victim, a player, a possible target, or a potential danger). Similar to this, how other nations see Pakistan's digital identity may have an effect on their strategic decisions and, ultimately, Pakistan's national security. We may better understand the function of norms by doing a constructivist study. Because there are no universally recognized principles in the field of cyberwarfare, the conflict there is tumultuous and complicated. States often use their manufactured interpretations of current international law and norms to support their aggressive or defensive actions. Pakistan may more effectively anticipate and react to challenges by comprehending these normative systems.

Additionally, constructivism's emphasis on ideational rather than material aspects might provide insight into the dynamics of soft power in information warfare. Ideas, belief systems, and public opinion may all be targeted in addition to the actual physical infrastructure. It is essential to comprehend how these intangible factors may be controlled and how they may affect national security. The constructivist perspective emphasizes that information warfare is a multilateral problem, including international systems and the larger international community, rather than merely a bilateral one between Pakistan and a specific state or non-state actor. Thus, it emphasizes the significance of international discussion and collaboration in resolving this problem.

Strategic Information Warfare Techniques

Cyber Attacks and Intrusions refer to malicious activities carried out by individuals or groups targeting computer systems, networks, and information. These attacks aim to disrupt operations, steal sensitive data, gain unauthorized access, or cause damage to digital infrastructure. Cyber-attacks have become increasingly prevalent with the rise of digitalization and connectivity. There are various types of cyber-attacks. The most common types include Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, Man-in-the-Middle (MITM) attacks, phishing attacks, malware attacks, ransomware attacks, SQL injection attacks, and more (Fortinet, 2023). Each type of attack employs different techniques to exploit vulnerabilities and achieve its objectives.

The year 2020 witnessed several significant cyber-attacks. Some notable incidents included ransomware attacks targeting organizations like Toll Group and Marriott International (Arielle, 2021). Ransomware attacks involve encrypting data and demanding a ransom for its release. These incidents highlight the financial impact and operational disruptions caused by cyber-attacks. In a recent incident, Russian cybercriminals launched a global ransomware attack affecting various organizations. The latest incident had a broad reach, including several sectors such as enterprises, institutions, and government entities. Several important entities fell prey to the cyberattacks, encompassing federal institutions in the United States, state agencies in Louisiana and Oregon, state governments in Minnesota and Illinois, and notable commercial corporations such as the BBC, British Airways, Aon, and The Boston Globe (Jennifer and Sean, 2023). The current inquiry aims to evaluate the magnitude of the breaches and comprehensively analyze their effect and repercussions.

Disinformation and propaganda are closely linked concepts that entail intentionally disseminating inaccurate or deceptive information to manipulate public sentiment or attain particular objectives. It is worth mentioning that misinformation, disinformation and propaganda are interchangeably used despite their distinct meanings. Misinformation may be defined as disseminating inaccurate or distorted information that contradicts widely accepted truths. Conversely, misinformation pertains especially to the deliberate dissemination of inaccurate information. Propaganda, on the other hand, refers to the deliberate transmission of frequently biased or misleading information to advance a certain agenda or exert influence over public opinion (Andrew and Benjamin, 2020). In the contemporary day, characterized by the widespread use of social media and online platforms, the significance of these phrases has been further amplified due to the expeditious dissemination of information.

The ramifications of the extensive proliferation of deception can have significant implications. This phenomenon could result in several outcomes, including the decline of trust in traditional institutions, impacts on political thoughts, the emergence of societal rifts, and the potential subversion of democratic practices. Various players may coordinate disinformation campaigns, including state-sponsored groups, political organizations, or people with malevolent intent. These actors may have many aims, including influencing electoral outcomes, fostering social unrest, or promoting certain ideological agendas. In light of the increasing prevalence of misinformation, it has become crucial to devise efficacious approaches to counteract its dissemination and alleviate its consequences.

Mitigating issues presented by misinformation necessitates the active engagement of many parties. The promotion of news literacy among individuals and the implementation of regulations that foster openness and accountability in the transmission of information may be significantly facilitated by governments. The news business also bears a duty in this regard since it should prioritize the production of journalism of high caliber, engage in fact-checking, and rectify any instances of misinformation to the best of its ability. Through collaborative efforts, it is possible to address the problem of misinformation and uphold the authenticity of information within our societal framework.

Technology companies can invest in tools and algorithms to detect and mitigate the spread of disinformation on their platforms. Educational institutions can prioritize news literacy education, teaching critical thinking skills, and promoting media literacy. Individuals should diversify their news sources, fact-check information before sharing, and cultivate a healthy skepticism towards online content.

Social Engineering and Psychological Operations are interconnected concepts that involve manipulating individuals or groups through psychological tactics to gain unauthorized access, influence behavior, or achieve specific objectives. Social engineering refers to the exploitation of human psychology rather than technical hacking methods to deceive individuals and gain unauthorized access to physical spaces, systems, or sensitive information. It often involves tactics such as impersonation, phishing, and pretexted phone calls to manipulate individuals into disclosing confidential information or performing specific actions (John, 2022). Social engineering attacks target human vulnerabilities and exploit traits like trust, curiosity, and deference to authority. These attacks can occur both offline and online, and even with robust security measures, a skilled social engineer can find ways to bypass them (Manfred, 2021).

Cybercriminals leverage various psychological triggers to increase the effectiveness of social engineering attacks. They exploit factors such as reciprocity, scarcity, authority, consistency, liking, and consensus, as outlined in Cialdini's Six Principles of Persuasion. Understanding these triggers can help individuals and organizations recognize and guard against social engineering tactics. By preying on human tendencies and emotions, social engineers manipulate victims into making decisions that may not be in their best interests (Christopher, 2021).

In addressing social engineering attacks, it is imperative to employ a comprehensive strategy encompassing several dimensions. Organizations should invest in employee training and education to raise awareness about social engineering tactics and the importance of skepticism and verification. Implementing strong security measures, including multi-factor authentication and regular security updates, can also help mitigate the risks. Individuals should develop a critical mindset, be cautious of unsolicited requests for information, and practice good password hygiene. Collaboration between organizations, technology providers, and cybersecurity experts is essential to develop effective countermeasures against social engineering (Jayanth, 2021).

Information warfare incidents involving Pakistan have been a subject of discussion due to the complex dynamics in the region. India has been implicated in employing disinformation techniques to discredit Pakistan and hinder its diplomatic ambitions. Non-governmental organizations, such as "DisInfo Lab," have revealed India's extensive disinformation campaign, which utilizes fake news media outlets to spread false information across multiple countries. This campaign includes the dissemination of anti-Pakistan propaganda through various channels, including UN-affiliated organizations (Saleem, 2022).

Cybersecurity and the risks associated with cyber warfare have become increasingly significant in modern warfare. Pakistan, like other countries, faces challenges in determining its position in the cyber domain and addressing cyber threats to national security. The country has taken steps to build capacity and raise awareness but still faces legislative gaps and vulnerabilities (Basma, 2022).

Information warfare has become a critical aspect of national security, posing challenges due to technological advancements. India, along with its allies, is utilizing social media platforms to fuel disinformation campaigns aimed at harming the interests of rival countries, including Pakistan. These campaigns involve the dissemination of propaganda, fake news, and deep fakes through social media channels. Evidence-based research has shed light on India's organized disinformation campaign aimed at damaging Pakistan's international image. This campaign involves the operation of a vast information weaponization network from India, disseminating pro-India and anti-Pakistan content through fake websites and resurrected organizations and individuals. The target audience includes policymakers in the EU and the UN (Raashed, 2020).

Pakistan's National Security Policy places a focus on the economy (Khalid, 2022), and therefore any disruptions to this via SIW can directly impact its national security. Strategic Information Warfare (SIW) possesses the capacity to incite political instability, primarily through means of disseminating disinformation and propaganda. The aforementioned phenomenon can substantially influence decision-making processes, undermine the integrity of political systems, and destabilize governments. The presence of the Security Intelligence Wing (SIW) in Pakistan can potentially exacerbate the intricate political dynamics, considering the country's preexisting problems posed by several opponents.

In addition, it is essential to note that SIW extends beyond political manipulation and has the potential to impact essential infrastructures such as electricity grids, communication networks, and transportation systems, leading to significant disruptions within society. Due to the ongoing development of Pakistan's cybersecurity architecture, it continues to exhibit susceptibility to various attacks. Cyber warfare has emerged as a significant worldwide concern, with notable instances such as the Stuxnet virus and the WannaCry epidemic, which have demonstrated considerable dangers to national security on an international scale (Basma, 2022). In addition to its physical ramifications, SIW can exert significant psychological effects, inducing anxiety, perplexity, and skepticism throughout the general populace. The manipulation of cultural views, the fostering of divides, and the incitement of unrest can harm society's stability, directly impacting national security. In Pakistan, where challenges are already posed by guerrillas, subversive elements, and insurgents, the adoption of SIW (Special Intelligence Wing) can potentially exacerbate the erosion of social stability.

Pakistan has had difficulties arising from hybrid warfare in the past, and the increasing risks associated with cyber warfare contribute to the situation's intricacy (Zafar, 2020). Despite several efforts to increase awareness and enhance capabilities, it is evident that more comprehensive measures are necessary to address these complex challenges adequately. Ensuring the proactive reinforcement of cybersecurity defenses and the augmentation of resilience are paramount in safeguarding national security and social well-being. The country's national security policy, while focusing on economy and non-traditional security, also needs to address systemic shortcomings and governance weaknesses to effectively combat the implications of SIW (Zaki, 2022). These consequences collectively underline the crucial need for a robust, dynamic strategy to counter the implications of Strategic Information Warfare on Pakistan's national security. In order to address this problem effectively, it is imperative to adopt a comprehensive strategy incorporating technology innovation, regulatory measures, and strong international collaboration.

Countermeasures and Mitigation Strategies

National policies and legal frameworks are crucial in the ongoing effort to combat Strategic Information Warfare. These instruments are vital in reducing the risks of such warfare and enacting truly effective remedies. Implementing robust legislative frameworks for the prosecution of cybercrimes, the protection of critical infrastructure, and the preservation of digital rights assumes paramount importance as indispensable measures in the defense against sophisticated information warfare (SIW) (Ankit, 2020). It is a positive development to observe nations implementing tangible measures by establishing precise legislation about cybersecurity, cybercrime, and data protection. This trend signifies a growing recognition of the need for robust legal frameworks in strengthening our defenses against cyber threats.

A comprehensive cybersecurity infrastructure is a crucial element in combating SIW. This encompasses both tangible and virtual remedies. Protecting sensitive information from unauthorized access is paramount, necessitating the utilization of secure servers and data centers on a physical level. In the realm of digital technology, it is imperative to prioritize the implementation of safe software and the deployment of sophisticated threat detection systems in order to identify and prevent cyber-attacks effectively. By allocating resources toward implementing extensive cybersecurity protocols, we may enhance our ability to withstand and respond to the intricate and constantly changing threats presented by Strategic Information Warfare. National Critical Infrastructure Protection programs and a vibrant cybersecurity ecosystem are also essential components of a comprehensive cyber defense strategy. A proactive approach to cyber threat detection and response, including national incident response and recovery plans, could help to minimize damage from cyberattacks (Ankit, 2020).

Educating the public about the risks of Strategic Information Warfare and promoting good cyber hygiene can be an effective mitigation strategy. Cybersecurity awareness programs can educate the public about the potential risks and safeguards against cyber threats, promoting a culture of cyber resilience. This includes teaching individuals how to identify and protect themselves from common threats such as phishing and malware attacks.

Given the transnational nature of cyber threats, international cooperation is crucial for effective countermeasures. Several initiatives are promoting such cooperation, such as the Global Cybersecurity Agenda by the International Telecommunications Union (ITU), focusing on legal, technical, organizational, capacity-building, and cooperation pillars. Collaboration with global partners can lead to the exchange of best practices, sharing of threat intelligence, and the joint enforcement of cybercrime laws. Collaborative governance, involving public, private, and societal actors, can enhance policy design and service delivery in cyber defense (Agnes and Sara, 2019).

All these countermeasures and mitigation strategies can help nations to tackle the threats from Strategic Information Warfare. The successful implementation of these measures requires a comprehensive approach, encompassing policy changes, infrastructural improvements, public awareness, and global cooperation.

Pakistan as Case Study

Information warfare (IW) in the South Asian context is an evolving domain of conflict that comprises both state and non-state actors utilizing information for offensive and defensive purposes. The focus of IW is not merely on conventional military engagements but also on the manipulation of information to shape public opinion, create confusion, and achieve strategic objectives.

One aspect of IW in South Asia is the application of "gray zone warfare," a term that refers to conflict situations that exist between conventional definitions of peace and war (Tahir, 2022). Gray zone tactics involve non-kinetic dimensions such as hybridity, soft power, and ambiguity. Although the study primarily focuses on Russia, China, and Iran as practitioners of this style of warfare, it notes that South Asia is also experiencing gray zone warfare.

In the specific context of India and Pakistan, the implementation of Network Centric Warfare (NCW) is changing the dynamics of conflict. India's pursuit of NCW, which seeks to integrate all aspects of warfare for increased speed, responsiveness, and combat effectiveness, is seen as a challenge to strategic stability in the region, especially given the country's Cold Start Doctrine that aims for swift military action.

Furthermore, the increasing utilization of social media as a tool for shaping narratives is a significant aspect of IW in the region. As the age of information continues to evolve, the strategic use, collection, analysis, alteration, and dissemination of information are becoming central to military and political objectives.

However, the effectiveness of SIW as a policy instrument is questioned, especially in the Indo-Pakistan context, due to its military nuances, which can hinder its application in dynamic sociopolitical contexts. Ultimately, SIW in the South Asian context is multi-faceted, encompassing traditional military strategies, the manipulation of information, and the strategic use of social media. Despite its potential effectiveness, it also poses significant challenges, both ethical and practical, that must be addressed to prevent escalation of conflicts and maintain regional stability.

The rivalry between India and Pakistan has expanded into the digital sphere with the increasing use of Strategic Information Warfare tactics. India utilizing digital platforms, notably Twitter, to wage information campaigns against Pakistan (Shabir, 2021). This was evident during the aftermath of the Pulwama attack and subsequent surgical strikes, where thousands of tweets were analyzed, revealing a pattern of overwhelming support within respective national hashtags and criticism within the opposing country's hashtags.

Furthermore, a broader strategy called Fifth Generation Warfare (5GW) is employed, incorporating hybrid tactics like disinformation campaigns. For instance, an extensive Indian network has been reportedly involved in information weaponization against Pakistan, targeting international institutions like the EU and UN since 2005 (Raashed, 2020). This disinformation network operates through fake websites, resurrected organizations, and individuals spanning across 68 countries.

To summarize, the India-Pakistan rivalry in the sphere of IW involves the strategic use of digital platforms, disinformation campaigns, and social media manipulation to gain an advantage. In this context, the engagement in digital warfare reveals the broader political, social, and military issues underlining the India-Pakistan relationship. It is evident that the escalating tension between these nations calls for counterstrategies to protect their national interests and maintain regional stability.

The role of external actors and proxy warfare in Pakistan is multifaceted and complex, involving state and non-state actors, military strategies, and geopolitical considerations. A proxy war, at its core, is an armed conflict between two states or non-state actors, instigated or conducted on behalf of other parties not directly involved. For a conflict to be characterized as a proxy war, it is required that a durable association exists between external players and the warring parties, typically encompassing financial backing, military instruction, or material aid. The comprehension of proxy conflicts and their resultant ramifications assumes paramount importance due to the substantial obstacles they provide to post-conflict stability, demobilization efforts, and the successful reintegration of former soldiers (Tahir, 2022).

The current events in Afghanistan, including the seizure of power by the Taliban, have introduced more intricacy to the involvement of external entities and the use of proxy warfare. There is mounting apprehension over the possibility of Afghanistan persisting as a theatre for proxy conflict, wherein various actors may forge alliances with the Taliban and other external entities (Aisha, 2020). The historical antagonism between India and Pakistan engenders the potential for an escalated proxy conflict between the two nations, particularly in light of India's aversion towards the Taliban.

Therefore, the involvement of external parties and the utilization of proxy warfare in Pakistan are intricately linked to broader regional security dynamics, characterized by a combination of strategic objectives, political competition, and military operations. Its intricacy and sensitivity characterize the current situation, requiring meticulous examination and strategic maneuvering to preserve regional stability and promote peaceful coexistence. It has both immediate and long-term implications for the stability and security of the region. Understanding these dynamics is critical for any attempts to resolve conflicts and build sustainable peace.

Information warfare has become increasingly significant in recent years; especially as technological advancements continue to reshape the landscape of modern warfare. As it relates to Pakistan, there are several lessons that can be learned from past experiences, and implications for the future. The first lesson learned is the importance of building a robust cyber security architecture. While Pakistan has initiated steps to raise awareness and build capacity among the public regarding cybersecurity, it still faces challenges in establishing a comprehensive framework to address the broad range of cyber threats (Basma, 2022). The instances of cyber warfare such as the Stuxnet virus attack on Iranian nuclear facilities and the WannaCry outbreak serve as important reminders of the risks that cyber threats pose to national security.

Another key lesson learned from the past is the importance of developing capabilities in the field of information technology and artificial intelligence (AI). Despite limited technological and industrial development, Pakistan aims to keep pace with global military trends, including advancements in AI. However, developing countries face significant challenges in establishing a strong scientific and technological foundation (Talat, 2021).

In constructivist lens, the future implications of information warfare are poised to play an increasingly dominant role in conflict scenarios. Modern conflicts are being fought on two fronts: the physical dimension and the narrative dimension shaped by traditional and social media (Aisha, 2020). Pakistan, like other countries, will need to navigate this complex environment where influencing opinions, wielding soft power, and destabilizing governments can be achieved through the strategic use of information (Saleem, 2021). This perspective underscores the imperative for the development of robust countermeasures that will safeguard against forthcoming disinformation campaigns, emphasizing the role of social constructivism in shaping both the perception of and responses to information warfare in the years ahead.

Finally, the increased cooperation between Pakistan and China, particularly in military and non-military aspects, has repercussions for the dynamics of information warfare in the region (Sushant, 2021). This suggests a changing strategic landscape that Pakistan will need to consider in its approach to information warfare.

Pakistan, like many other nations, is grappling with the challenges posed by the evolution of information warfare. Learning from the past, building cyber resilience, investing in advanced technology, and preparing for the increasing importance of information warfare in conflicts are key considerations for Pakistan moving forward.

Conclusion, Recommendations and Future Direction

A nation-state or commercial organization must manage all of its resources in a coordinated and synchronized way in order to govern the information environment, achieve and sustain a competitive edge, and increase power and influence. In both the physical and virtual realms, governments and companies may employ SIW offensively and defensively. SIW countermeasures do not have to consist of in-kind; they might be asymmetrical, low-tech, high-tech, or none. Even if the nomenclature may change, SIW will progress beyond its infant stage and become mainstream in the next twenty years. SIW is all about coordinated, synchronized connections and talents. Utilizing all of its resources in a coordinated and synchronized way, its business uses all of its resources to get the greatest competitive advantage feasible. So that as much expertise and power as possible may be used, a nation can call upon its friends and coalition partners, and a corporation can rely upon its business and suppliers' partners. Pakistan is now going through a crucial period as the country faces enormous internal and external problems. It is not a choice to become numb and defiant. Pakistan would need to develop a thorough Counter SIW Strategy to counter all SIW campaigns carried out by both insiders and foreigners. Even a complete strategy involving academics and the media might fail if they do not present a united front in the face of internal and foreign dangers. Pakistan cannot afford to let its guard down in relation to the cyber danger to its nuclear assets since it is a nuclear weapon state. Therefore, Pakistan must implement all essential precautions to guarantee that its nuclear weapons continue functioning as needed.

Based on the given context and the increasing importance of information warfare in today's interconnected world, the following policy recommendations can be suggested for Pakistan in strategic information warfare: Given the growing prevalence of cyber threats, it is essential for Pakistan to invest heavily in strengthening its cybersecurity architecture. This involves not only implementing advanced cybersecurity technology but also developing a comprehensive legislative framework to combat cyber threats.

The effective use of cutting-edge technology, such as artificial intelligence and machine learning, is a pivotal element within information warfare. In order to adequately tackle the complexities associated with information warfare, Pakistan must emphasize allocating resources towards technology research and development. Concurrently, it is imperative to prioritize the improvement of technology education in order to foster a proficient workforce that possesses the necessary competencies to navigate the ever-evolving environment effectively.

Per its overarching National Security Policy, Pakistan should consider developing a distinct policy centered on information warfare. A comprehensive policy should have offensive and defensive components, delineating the strategic and tactical approach of the nation in addressing these challenges. Given the increasing frequency of misinformation operations, Pakistan must adopt effective methods to counter these deliberate attempts. The mitigation of the impact of misinformation efforts may be facilitated by enhancing capacities in identifying and exposing such campaigns, with the promotion of media literacy among the general public.

Due to the worldwide scope of information warfare, it is imperative to have a comprehensive international approach to addressing this phenomenon. Pakistan must engage in collaborative efforts with foreign partners to formulate collective strategies to counter this particular type of warfare. This may entail pushing for the creation of international governance institutions and policy frameworks about information warfare. In addition, it is imperative to emphasize the need for increasing knowledge regarding information warfare among civilian leaders and the general public to cultivate a complete comprehension of its potential dangers.

In order to enhance the resilience of national security and promote research within the realm of information warfare, it is advisable to propose a multifaceted strategy. By utilizing theoretical frameworks such as the "Intermediate School Theory" and the S.E.C.R.E.T model, it is possible to get significant insights that can contribute to the improvement of resilience against information warfare, with a focus on the unique context of Pakistan.

In addition, future research endeavors must prioritize the comprehensive examination of the impact of Emerging Disruptive Technologies (EDTs) on information warfare, encompassing analysis of possible vulnerabilities and defensive strategies. Furthermore, it is imperative to conduct continuous research and examination of the notion of resilience, particularly within the framework of dynamic security threats, climate change, catastrophes, and societal dimensions.

The field of information warfare and cyber threats undergoes fast evolution, requiring ongoing monitoring of the threat environment and timely adjustment of plans and resilience measures. By integrating these methodologies, Pakistan has the potential to enhance its national security resilience against information warfare while simultaneously facilitating innovative research in this crucial domain.

Reference List

Agnes, B. and Sara, S. (2019). Regulating Collaboration: The Legal Framework of Collaborative Governance in Ten European Countries. International Journal of Public Administration. Taylor & Francis Online. Available at:
https://www.tandfonline.com/doi/full/10.1080/01900692.2019.1658771

Aisha, S. (2020). Information Warfare: The Future of Conflict in South Asia. Pakistan Defense. Available at:
https://pdf.defence.pk/threads/information-warfare-the-future-of-conflict-in-south-asia.686357/

Andrew, M. G. and Benjamin, A. L. (2020). Misinformation, Disinformation, and Online Propaganda. Cambridge University Press. Available at:
https://www.cambridge.org/core/books/social-media-and-democracy/misinformation-disinformation-and-online-propaganda/D14406A631AA181839ED896916598500

Ankit, F. et al. (2020). Follow the leaders: How governments can combat intensifying cybersecurity risk. McKinsey & Company. Available at:
https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks

Antoine, L. (2022). Why Pakistan’s first national-security policy matters for future regional stability, IISS. Available at:
https://www.iiss.org/online-analysis/online-analysis/2022/02/why-pakistans-first-national-security-policy-matters-for-future-regional-stability/

Arielle, W. (2021). 10 of the biggest cyber-attacks of 2020. TechTarget. Available at:

https://www.techtarget.com/searchsecurity/news/252494362/10-of-the-biggest-cyber-attacks

Basma, K. (2022). Emerging Cyber warfare threats to Pakistan. Strategic Vision Institute. Available at:
https://thesvi.org/emerging-cyber-warfare-threats-to-pakistan/

Cameran, A. (2021). Defining cyberwar: towards a definitional framework. Defense & Security Analysis. Taylor & Francis Online. Available at:
https://www.tandfonline.com/doi/full/10.1080/14751798.2021.1959141

Christopher, H. (2021). Social Engineering and Psychology. Human Hacking, Psychology Today. Available at:
https://www.psychologytoday.com/us/blog/human-hacking/202102/social-engineering-and-psychology

Farooq, K.K. (2021). Pakistan's national security complexities, Centre for Strategic and Contemporary Research. Available at:
https://cscr.pk/explore/themes/defense-security/pakistans-national-security-complexities/

Fortinet. (2023). Types of Cyber Attacks. Available at:
https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

Ganguly, S. (2022). What Pakistan's new National Security Policy leaves out, Foreign Policy. Available at:
https://foreignpolicy.com/2022/02/02/pakistan-national-security-policy-internal-challenges/

Jacob, R. (2020). Strengthen National Security: National Resilience Philosophy Approach - National Security research abstract. Varna Free University. Available at: https://www.researchgate.net/publication/339935568_STRENGTHEN_NATIONAL_SECURITY_NATIONAL_RESILIENCE_PHILOSOPHY_APPROACH_-_National_Security_research_abstract

Jayanth, K. (2021). Motivational and Psychological Triggers in Social Engineering. SSRN. Available at:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3750474

Jennifer, K. and Sean, L. (2023). A ransomware attack is hitting schools, businesses and government agencies. Here's what you should know. CNN Business. Available at: https://edition.cnn.com/2023/06/16/tech/clop-ransomware-attack-explainer/index.html

John, F. (2022). Social engineering: Definition, examples, and techniques. CSO. Available at:

https://www.csoonline.com/article/571993/social-engineering-definition-examples-and-techniques.html

John, L. (2022). What is information warfare and how pervasive is it? World Economic Forum. Available at:
https://www.weforum.org/agenda/2022/04/what-is-information-warfare-and-how-pervasive-is-it/

Khalid, Z. (2022). Examining the national security policy of Pakistan 2022-2026, Centre for Strategic and Contemporary Research. Available at:
https://cscr.pk/explore/themes/defense-security/examining-the-national-security-policy-of-pakistan-2022-2026/

Manfred, C. (2021). PsyOps: Deep Dive into Social Engineering Attacks. Tevora. Available at:
https://www.tevora.com/threat-blog/psyops-part-1-of-2-deep-dive-into-social-engineering-attacks/

Molander, R.C. et al. (1998). Strategic information warfare rising, RAND Corporation. Available at:
https://www.rand.org/pubs/monograph_reports/MR964.html

Molander, R.C., Riddile, A. and Wilson, P.A. (1996). Strategic information warfare: A new face of war, RAND Corporation. Available at:
https://www.rand.org/pubs/monograph_reports/MR661.html

Nick, B. (2018). Information Warfare Past, Present, and Future. Real Clear Defense. Available at:
https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_and_future_113955.html

Raashed, M. (2020). The ‘indian chronicles’: India’s Information Weaponisation against Pakistan, Centre for Strategic and Contemporary Research. Available at:
https://cscr.pk/explore/themes/defense-security/the-indian-chronicles-indias-information-weaponisation-against-pakistan/

Rabia, A. (2022). Pakistan’s new National Security Policy: A step in the right direction, Atlantic Council. Available at:
https://www.atlanticcouncil.org/blogs/southasiasource/pakistans-new-national-security-policy/

Robert, R. (2017). Information warfare, obo. Available at:
https://www.oxfordbibliographies.com/display/document/obo-9780199791279/obo-9780199791279-0024.xml

RSIS. (2014). Rethinking Information and Cyber Warfare: Global Perspectives and Strategic Insights. Nanyang Technological University. Available at: https://www.rsis.edu.sg/rsis-publication/idss/rethinking-information-and-cyber-warfare-global-perspectives-and-strategic-insights/?doing_wp_cron=1688231134.8015689849853515625000

Saleem, M. (2022). Indian disinformation operations against Pakistan and its implications, Centre for Strategic and Contemporary Research. Available at: https://cscr.pk/explore/themes/defense-security/indian-disinformation-operations-against-pakistan-and-its-implications/

Shabir, H. et al. (2021). Analyzing the State of Digital Information Warfare Between India and Pakistan on Twittersphere. Sage Journals. https://journals.sagepub.com/doi/full/10.1177/21582440211031905

Shoaib, B. (2022). Pakistan's new security challenges. Pakistan Today. Available at: https://www.pakistantoday.com.pk/2022/03/27/pakistans-new-security-challenges/

Sushant, S. (2021). The Challenge of a Two-Front War: India's China-Pakistan Dilemma. Stimson, Asia & Indo-Pacific. Available at: https://www.stimson.org/2021/the-challenge-of-a-two-front-war-indias-china-pakistan-dilemma/

Tahir, M. A. et al. (2022). Understanding Gray Zone Warfare from Multiple Perspectives. World Affairs, Sage Journals. Available at: https://journals.sagepub.com/doi/10.1177/00438200221141101

Talat, M. (2021). Arms race and emerging global military trends. The Express Tribune. Available at: https://tribune.com.pk/story/2326510/arms-race-and-emerging-global-military-trends

William, R. G. et al. (2017). Information warfare in an information age. National Defense University Press. Available at: https://ndupress.ndu.edu/Media/News/Article/1130649/information-warfare-in-an-information-age/

Zafar, N. J. (2020). Pakistan's National Security Hybrid Warfare Challenges & Countermeasures. Center of Pakistan and International Relations. Available at: https://www.researchgate.net/publication/340514708_Pakistan%27s_National_Security_Hybrid_Warfare_Challenges_Countermeasures

Zaki, K. (2022). Examining the National Security Policy of Pakistan 2022-2026. Centre for Strategic and Contemporary Research. Available at:
https://cscr.pk/explore/themes/defense-security/examining-the-national-security-policy-of-pakistan-2022-2026/