SOCIAL SCIENCE REVIEW ARCHIVES
https://policyjournalofms.com
ISSNOnline:3006-4708
ISSNPrint: 3006-4694

Hybrid Conflict in the 21st Century: Pakistan's Security Dilemmas and Responses

Dr. Muhammad Hatim [1], Dr. Adeel Irfan [2], Elahi Umar Ranjha [3], Haroon Shah[4], Muhammad Ahmad [5]

[1] Assistant Professor Department of Politics and International Relations University of Sargodha
muhammad.hatim@uos.edu.pk
[2] Assistant Professor Department of politics and international relations University of Sargodha
adeel.irfan@uos.edu.pk
[3] Scholar, Department of politics and international relations University of Sargodha
elahiranjha302@gmail.com
[4] Scholar, Department of politics and international relations University of Sargodha
haroonshah444@gmail.com
[5] Scholar, Department of politics and international relations University of Sargodha
awanahmad881@gmail.com

DOI: https://doi.org/10.70670/sra.v3i2.684

Abstract:

Hybrid warfare combines traditional and modern tactics, creating security challenges for every country. In Pakistan, army warfare poses a major threat. This danger blends with politics, economics, and cyber and information warfare. Together, these create a hybrid threat. This work is focused on understanding the different strategies employed in the hybrid war against Pakistan, determining the weak points of defense, governance, and the society's political systems. Utilizing the investigation of historical cases, analysis of geopolitical factors, and security frameworks, the study aims to identify the factors through which hybrid threats have effects on Pakistan's independence, solidarity as a nation, and levels of internal peace. The research discusses the sources of hybrid warfare with their character and maps out the options for countering the threats that Pakistan has - the instruments of military, intelligence, or policy. Finally, the paper considers the vulnerability of the technological progress that could be the source of the increase of the local national threat the most and the available alternatives that could help in managing the risks of the hybrid warfare. The discovery of this tidal wave is expected to give a complete picture of how to make Pakistan's national strategy in the security realm impeccable and how to fight against all complicated hybrid threats efficiently.

Keywords: Hybrid Warfare, National Security, Pakistan, Vulnerabilities, Security Strategies, Geopolitics, Information Warfare, Cyber Warfare, Conventional and Unconventional Tactics, Military Preparedness.

Introduction

1.1 Background of the Study

The prevalence of hybrid warfare as the most intricate and tricky issue for keeping peace and security in the world has been specifically pointed at for the states that are very volatile like the countries of South Asia. The idea of hybrid warfare refers to the deliberate combination of the military, political, economic, cyber, and informational tactics, allowing the attackers to exploit a target state's vulnerabilities without provoking a conventional war (McCallister, 2017). The aim of hybrid warfare is merely not to win the battle, but to create a situation wherein the enemy's political establishments get eroded, their people get disjointed and lastly, the enemy gets relieved of its sovereignty, not obviously but skillfully and persistently. In this context, the concept of hybrid warfare is very much relevant for Pakistan, where the country has, because of its special geopolitical location, unresolved conflicts with its neighboring states and internal socio-political issues, multiple vulnerabilities to this type of attack.

Hybrid warfare is a kind of warfare without a fixed, constant, or unchangeable definition, due to its constant change of form over time, but in essence, it means that a combination of conventional and non-conventional instruments is used simultaneously to carry out political and military aims. It is used not only by various organizations and groups but also by individuals who are not related to the state to achieve more than one goal. The activities involved might be disinformation campaigns, cyber-attacks, economic coercion, proxy warfare, etc. which are performed simultaneously so that at the end the country is taken with a surprise and not necessarily with a war declaration. Terrorism frequently is a part of hybrid warfare especially in the global context, and it is done to engage the emotional and psychological side of the targets and make the task of the terrorists easier (Innes & Mace, 2017).

The general method is often seen as the process with the following elements - disinformation, cyberattacks, economic pressure, deployment of irregular armed groups, and use of regular forces. Typical activities of hybrid warfare include military and non-military combinations, both open and hidden, including disinformation, cyberattacks, economic pressure, etc. (NATO, 2019). The convergence of strategies makes the situation extremely difficult to discern the place of the origin of the attack, to react properly, or to gather international forces for action.

The fact that hybrid warfare continues to change is a result of the overall change in global military principles over the last thirty years or so that has its roots mainly in technology. In the past, the military was traditionally divided into two different categories namely the conventional and nuclear sectors. Nevertheless, the asymmetrical threats, especially after 9/11, not only those but also the evolution of the global security situation due to non-state actors' increasing influence on the global security landscape influenced have emerged the new era where international security dynamics have begun to be shaped by non-state actors and hybrid tactics (Hoffman, 2007). The occurrences in Iraq, Afghanistan, Ukraine, and Syria have shown that hybrid war can challenge the military of the most advanced countries when using guerrilla tactics, cyber warfare, knowledge manipulation, and economic disruptions all together. The highly publicized crisis from Crimea, when a report of Russian misinformation is very often mentioned first and foremost, is a prime example of the hybrid war issue (utilizing disinformation).

In South Asia, Pakistan remains one of the most significant stakeholders in regional security dynamics for the sheer reason of its location close to countries such as India, China, Afghanistan, Iran, in addition to having had a historical and strategic partnership with the United States and China. Pakistan's national security framework includes military deterrence. It also considers social, cultural, economic, educational, and ideological factors. Recently, Pakistan has faced many security issues. These include terrorism, insurgency, sectarian violence, and foreign-backed sabotage. Right now, these challenges are increasingly seen as hybrid warfare incidents. One of the examples is when social media platforms are used for the dissemination of disinformation, cross-border support of insurgent groups and illegal intrusion in cyber space, which in a comprehensive approach become various shades of hybrid threats designed both to disrupt Pakistan’s internal environment and portray it as an isolated international outcast (Ahmed, 2017).

The hybrid warfare concept is especially functional when applied to a country like Pakistan, which is divided for numerous internal issues, which may be on ethnic, religious, and/or political sides, and thus can be made use of by the adversaries. Formerly, the state of Balochistan and areas like Gilgit-Baltistan, along with mob-based sectarian feuds in major cities, were present throughout these areas, sometimes related to foreign manipulation and strategic game playing. These vulnerabilities can easily be aggravated by psychological operations that aim to split the people and create an atmosphere of distrust among them and media influence that exacerbates the situation. The battlefield of the narrative has now shifted to social media where not only can the false stories that are created by unfriendly actors be moved but also the societal division can be made even deeper (Giles, 2016). Moreover, if it is not accompanied by decisive counter-narrative strategies and reinforced with ineffective cyber defense capabilities, it only serves to intensify the negative effect of these hybrid tactics.

Economic destabilization is another critical aspect of hybrid warfare against Pakistan. Manipulation of trade relations, exploitation of international financial institutions, sanctions, and influence over foreign investment flows are examples of the tools used to cripple the economic backbone of the state. This issue is of utmost importance in the context of the China-Pakistan Economic Corridor (CPEC) on which physical and ideological attacks have been launched. CPEC, the epitome of Pakistan’s economic vision, being put at risk is a clear case of the intertwining of the kinetic and non-kinetic forms of war to inhibit growth and affect strategic decisions (Ahmed, 2017).

The hybrid threat concept has also been deeply affected by the growing importance of cyber warfare and espionage. Cyber espionage in the military, power grids, financial systems, and government databases is a concrete danger to the national sovereignty of a country. These intrusions are frequently of a non-evident nature or of a difficult-to-attribute nature so that the enemy can stay below the level at which a traditional military response is not appropriate (Giles, 2016). The cyber defense capabilities of Pakistan are in the initial stage of development, and this is why critical infrastructure of the country is at risk of being hacked into. The legal as well as diplomatic grey zones are where the hybrid warfare is very active as they do not require conventional responses such as military retaliation that are either impossible or counter-productive.

Hybrid warfare has become a very important aspect of national security in today's world of global security. The change in warfare has been so in-depth that it is not just the tangible that has been affected by intangibles, but also the local areas (U.S. National Intelligence Council, 2008). This new concept of national security does not only mean border protection but it also requires the integrity of the information, cyber resilience, macroeconomic stability, and social coherence security. Pakistan must, therefore, come up with security shifted policies and measures that guarantee it gives an appropriate answer to these challenges that affect the country more than one. A comprehensive approach that combines military preparedness with increased intelligence, cyber security, diplomatic agility, and public resilience is needed to meet the challenge (Mansoor, 2012).

1.2 Statement of the Problem

Pakistan is facing new types of threats. These are non-traditional and asymmetric. They are part of what we call hybrid warfare. These threats come from many areas. They include cyber attacks, propaganda campaigns, economic destabilization, and proxy wars. Pakistan has boosted its military and security. However, it remains unprepared for hybrid threats. Its approach remains scattered and reactive. Pakistan faces strategic risks due to no clear national strategy. There is also weak coordination between institutions. Plus, the public and policymakers lack awareness. Knowing the different hybrid warfare strategies used against Pakistan is key. It helps boost national resilience and develop a strong counter-strategy.

1.3 Research Objectives

This study aims to analyze how hybrid warfare affects Pakistan’s national security. It will also suggest policy recommendations to counter these threats. The specific objectives are:

1. To define and contextualize hybrid warfare in the global and regional security environment.
2. To identify and examine the key hybrid warfare strategies employed against Pakistan.
3. To explore Pakistan’s critical vulnerabilities in the face of hybrid threats.
4. To assess the existing national security mechanisms and their effectiveness in countering hybrid warfare.
5. To propose policy measures and strategic frameworks to enhance Pakistan’s defense against hybrid threats.

1.4 Research Questions

To reach these goals, the study will focus on these main research questions:

1. What constitutes hybrid warfare, and how is it different from traditional warfare?
2. What hybrid strategies have state or non-state actors used against Pakistan?
3. What are the key weaknesses in Pakistan's politics, society, economy, and cyberspace that leave it vulnerable to hybrid warfare?
4. How well do Pakistan’s national security policies handle hybrid threats? What responses are in place?
5. What reforms and policies can help Pakistan resist hybrid warfare?

1.5 Significance of the Study

This research sets itself apart from many others as its relevance could not be overstated in the security issues in this day and age. In case one had not the opportunity to watch the war that has shifted to other, non-traditional, battlefields like, for instance, cyberspace, information war, economic manipulation or psychological operations, the expertise in hybrid warfare tactics has emerged as a priority. However, for Pakistan, being in a strategically critical location and having adversary neighbors like India, Afghanistan, in general, hybrid warfare apart from many other risks possesses the military, socio-political and economic dimensions.

Not too familiar with such studies in South Asian discourse, this paper is pioneering in that it is one of the few sources that provide insights into South Asian countries' hybrid warfare. Although this method of warfare is not new to some Western military and strategic thinkers, it has been widely discussed in the context of the actions of Russia in Ukraine and Crimea, there is no literature that focuses on Pakistan's Southwest Asian region to help them understand the consequences and effects of hybrid warfare. This study has the significance of academic work and the strategic input for national security planning at the same level and it contributes to the current knowledge pool while involving a regional research project.

Hybrid warfare can be quite intricate by the fact that it employs various methods of both non-military and military nature including misinformation, cyber-attacks, diplomatic coercion, proxy warfare, and economic sabotage. Pakistan's situation is further made difficult due to the internal vulnerabilities it has like ethnic diversity, sectarian tensions, the existence of porous borders, and a vibrant social media landscape which make it an easy target for such techniques. The study aims at analyzing these vulnerabilities in a structured manner and offering equation countermeasures which can be implemented through institutional reforms, strategic communications, and intelligence coordination for the country.

Moreover, the study deals with the issue of the new forms of warfare triggered by the developments in technology. The use of AI, big data, and cyber weapons of today has brought a big revolution to the hybrid warfare tactics, and as such, states have to be able to change rapidly to the changes taking place. Pakistan with its limited technological preparedness and reactive policy mechanisms is mostly not geared enough to proactively handle such threats and many times is caught unawares. The research, therefore, focuses the spotlight on the necessity of the rebuilding of the national security strategy of Pakistan towards a more proactively hybrid-threat-encompassing doctrine.

Further, the results of this study help define the foreign policy of Pakistan in its relations with regional and global powers. Knowing that detractors of Pakistan have employed hybrid warfare has resulted in the ability to develop well-informed diplomatic strategies which can counteract these hostile actions and continue to maintain the country's international reputation and alliances. That it is to say, India's accused partaking of insurgent groups' support in Pakistan and a method to sour the view of the public through using international arena can be referred to as a hybrid type of conflict (Khan, 2020).

Apart from that, this study also has great implications for the civil society and the media. Civil society and media usually are those who face the brunt of psychological and information operations in hybrid warfare. One way to empower society to resist the distortion of facts and the manipulation of disinformation is by promoting media literacy and civic resilience. It leads to the strengthening of the democratic process and the integration of the nation in the face of the alien attempts of creating internal division.

Finally, the paper offers important information for military and defense planners too. Since hybrid warfare is a combination of war and peace, which is a very thin line, the military's old classic response preparedness is no longer enough. Only a prepared modern military doctrine that can predict and thwart online threats, control the narrative through media, and liquidate proxy elements can be the cornerstone of a hybrid warfare-specific strategy reaching beyond the traditional military framework and suitable to Pakistan. The research through the finding of patterns and studying the sample cases of hybrid warfare, brings on the transformation of the doctrine specifically designed for Pakistan.

1.6 Scope and Limitations of the Study

The scope of this study revolves around analyzing the strategies employed in hybrid warfare against Pakistan and identifying the country's corresponding vulnerabilities across various dimensions—military, cyber, political, economic, and social. The research focuses primarily on the post-9/11 period, as this era has seen a marked transformation in the nature of security threats to Pakistan, moving from conventional warfare to more ambiguous and non-linear forms of conflict.

The study investigates hybrid warfare threats posed mainly by state and non-state actors, with particular emphasis on India's use of psychological operations, cyber attacks, media propaganda, and proxy support to destabilize Pakistan. It also includes an assessment of hybrid tactics employed through international financial institutions, global media outlets, and diaspora networks. Furthermore, the research evaluates Pakistan's current response mechanisms, institutional preparedness, and strategic gaps in countering hybrid threats.

There are certainly several constraints one has to consider in order to establish an unbiased comprehension of the study's limits. The first one is that this study forbore the use of primary fieldwork or collecting classified intelligence data reasons of access and ethical constraints. It was the data from such sources as government documents, academic journals, news reports, and think tank publications that were the material the study relied on. They, however, could be not the closest ideas to what is being done in practice at present.

Second, the use of hybrid war as a hidden activity is a significant restriction in itself. Unlike traditional warfare, where the enemy and strategies are easily spotted, hybrid threats often carry out their activities in the so-called grey area. This makes it a considerable challenge to detect, measure, or analyze them in a comprehensive way. A piece about the attribution of cyber attacks or disinformation campaigns to a particular actor is still a problem and that could be one of the reasons for the lack of clarity in certain findings (Clarke &Knake, 2010).

Fourth, the study itself is restricted to one specific region—Pakistan and its surroundings. While global examples of hybrid warfare (for example, Russia in Ukraine or Israel's operations in the Middle East) have been cited as being useful for comparisons, yet Pakistan is the main focus of the analysis per se. In other words, the study's results may not be universally relatable to all the states that face hybrid threats.

Additionally, the study operates under time constraints and a specific academic framework, which restricts its ability to conduct in-depth longitudinal analysis. The dynamics of hybrid warfare are constantly evolving, influenced by technological innovation, political developments, and global events. Therefore, the study provides a snapshot of the current landscape rather than a definitive or predictive model.

Finally, the interdisciplinary nature of hybrid warfare—which spans military science, cyber security, political theory, international relations, and psychology—makes it difficult to address all aspects comprehensively within a single thesis. While the study attempts to integrate insights from multiple disciplines, its treatment of each may be somewhat limited by scope and academic expertise.

Literature Review and Theoretical Framework

2.1 Concept and Definitions of Hybrid Warfare

Hybrid warfare is an artful concept encompassing different regions and faces that mobilize traditional military operations with irregular tactics, cyber warfare, psychological operations, disinformation, economic pressure, and proxies to achieve the strategic goals of the enemy without traditionally declaring war. This type of warfare muddles the waters between war and peace, state and non-state actors, and physical and informational domains.

Hybrid warfare, according to Hoffman (2007), is the application of conventional weapons, irregular tactics, terrorists, and rogueries of the same kind of battle space at the same time. One advantage of employing this strategy is that the opposite side is able to use the weak points of regular armed forces for their own interests and thus obtain asymmetric advantages.

NATO (2010) holds that hybrid threats are those threats that "are caused by enemies, who have the competence to attack by applying simultaneously traditional and unorthodox methods in order to achieve their goals." Indeed, hybrid warfare lies in the tools used and in the way those tools are interrelated and put to use across different theaters.

- The entire spectrum of hybrid warfare includes:
- Propagandas of lies and phony stories blitzes
- Viruses planting in central control computer systems
- Recourse to non-state actors, militias, and terrorist groups
- Using economic pressure and distorting the market to gain protection
- Manipulations in diplomatic and legal fields (lawfare)
- Operations of the mind and propaganda

Many people refer to the 2014 Crimea annexation by Russia as an archetypal case of hybrid warfare, an approach that sees military methods intertwined with cyber hacking, disinformation, and other non-military actions so that the domestic conflict does not escalate (Galeotti, 2016). Hybrid warfare thus challenges the conventional security doctrines and calls for a response that is fully integrated and coordinated across not only the military but also the civil, cyber, economic, and diplomatic sectors.

2.2 Evolution and Global Trends of Hybrid Warfare

There are numerous historical records of these tactics. However, modern societies developed these strategies beyond recognition after the Cold War, with globalization, innovative technology, and digital communications causing significant change to warfare.

Evolution of Hybrid Warfare

- Cold War Period: The Vietnam, Afghanistan, and Latin American conflicts provide an excellent illustration of the employment of hybrid tactics where the superpowers, through proxies and the lik,e achieved their geostrategic goals without direct engagement.
- Post-9/11 Era: Non-state actors like Al-Qaeda and later ISIS utilized hybrid strategies by uniting terrorism with social media propaganda, financial networks, and territorial control (Kilcullen, 2009).
- Ukraine Crisis (2014): Russia's annexation of Crimea and operations in Eastern Ukraine demonstrated a sophisticated hybrid strategy that involved cyber-attacks, information warfare, unmarked troops (“little green men”), and the use of local proxies (Marten, 2015).
- China’s Grey Zone Tactics: China uses hybrid methods in the South China Sea by deploying fishing militias, cyber intrusions, and legal warfare to assert territorial claims without direct military conflict (Cordesman, 2019).
- Cyber and Information Warfare: The rise of digital platforms and social media has made information operations a central pillar of hybrid warfare. Fake news, deepfakes, and bot-driven propaganda campaigns are used to influence public opinion, polarize societies, and disrupt democratic institutions (Rid, 2020).

Global Trends

1. Increased Use by State and Non-State Actors: For instance, Russia, China, Iran, and North Korea, and to terrorist groups, are all using hybrid means as a part of their strategic frameworks.
2. Cyber Domain Expansion: Among the most significant means in hybrid warfare are cyber tools such as electronic elections agendas, data acquisition, and infrastructure disruption.
3. Artificial Intelligence and Big Data: AI-led data collection, emotional profiling, and targeted misguidance are some of the tools that are being used to become even more powerful in the process of hybrid warfare.
4. Targeting Democratic Societies: Because of their freedom of the press, civil liberties, and political pluralism, democratic societies are often more susceptible to hybrid threats, which can lead to electoral manipulation, unrest incitement, or the discrediting of institutions.
5. Multilateral Counter-Strategies: Both NATO and the EU are getting ready to stand up to hybrid warfare using plans like the sharing of intelligence, cybersecurity, and the empowerment of the public through moral and informative campaigns (NATO, 2015; EU Hybrid Fusion Cell).

2.3 Hybrid Warfare in the South Asian Context

Hybrid warfare refers to a combination of conventional warfare, unconventional or irregular warfare, and cyber operations employed together with other psychological and information-based strategies that accomplish political and military aims. With such a plethora of approaches, this model of warfare is uniquely suited for the use of the entire gamut of instruments of power and thus operates symmetrically with both conventional and non-military issues which occur in the cyberspace thus encouraging readiness in the fight against both elements and prepares for the future of asymmetric warfare. South Asia, primarily Pakistan, has been most susceptible to such forms of warfare, given the conflict with the neighboring countries of India and Afghanistan, which are ongoing, as well as the social, political, and security uncertainties of the region.

In South Asia, hybrid warfare has not only been adopted by both state and non-state actors but also has found camaraderie with them to gain strategic aims without actual combat. Pakistan, in particular, has been targeted by an array of hybrid techniques executed by enemies who use a combination of forceful military threats, secret operations, economic punishments, and neuro-linguistic programming (NLP) campaigns. The problems with India, including terrorism across the border, proxy wars, and information warfare, have been the most visible cases in the region of hybrid warfare. Also, Pakistan's pursuit in Afghanistan, as well as the Pakistan-India dynamic and the involvement of other regional players, have made the country easy prey for hybrid and proxy warfare.

Hybrid Warfare in South Asia: Tactics

Proxy Warfare: Both India and Pakistan have traditionally used non-state actors to achieve their political and military objectives in the region of Kashmir and other localities, which accordingly increased the complexity of a hybrid warfare situation.

Cyber Attacks: With cyber threats, the mode of cyber-physical systems' security is being increasingly utilized for this purpose. Pakistan has undergone cyber-physical attacks against its military, governmental, and financial institutions.

Psychological Warfare: Disinformation campaigns are widespread in South Asia, with adversarial actors utilizing social media platforms to manipulate public opinion and sow discord among citizens and political groups.

Economic Warfare: International sanctions and trade barriers, as well as manipulation of economic dependencies, are common tools of hybrid warfare. Pakistan has faced economic pressure from international entities that are influenced by its adversaries.

Use of Militants: Proxy militants and insurgent groups have been leveraged to destabilize regions, with support for militant activities often camouflaged as part of broader geopolitical strategies.

Hybrid warfare has been a significant challenge in South Asia because of the geopolitical chaos inherent within the region, the race of nuclear armament and the presence of numerous insurgent groups. The element of the leaders of the rival factions being able to make war seem peaceful, and meanwhile, it is happening in some areas that are uncontrolled by the government, added to the lack of efficient security within the region, bringing about the opportunity for the' effective employment.

2.4 Key Theories Supporting the Study

This research makes use of various theories that are of great importance for the study of hybrid warfare in the context of national security of Pakistan. These theories provide explicit ways of interpreting the acts of enemies and the other part show the enumerated weaknesses of the defense mechanisms of Pakistan.

2.4.1 Hybrid Warfare Theory (Frank Hoffman)

One of the main figures in the field, Frank Hoffman's Hybrid Warfare Theory, has made a major contribution to the reshaping of the conception of the current and upcoming warfare terrain through a comprehensive interpretation of the coexistence of the parties with and without the public power in their non-military and military operations. In his landmark publication, Hoffman states that hybrid warfare is defined as "a mixture of common and uncommon, regular and irregular, and information and psychological warfare."

Theory is a valid explanation for comprehending the adverse effects of hybrid warfare on Pakistan due to it being frequently hybridly fought, especially from India and non-state actors. There is a need for the security apparatus of Pakistan to deal with both common military threats and with the range of non-traditional security challenges such as terrorism, cyber-warfare, and psychological operations. In the view of Hoffman, hybrid warfare takes place in the space envisioned as armed and unarmed tactics combined, shaping a wider range of challenges that do not fit neatly into traditional defense or offense categories.

The main elements of Hybrid Warfare (according to Hoffman) are as follows:

- Multi-Domain Model: Simultaneous operations in hybrid warfare occur across different domains, such as cyber, air, land, and sea.
- Non-State Actors: Insurgents and militants are a significant part of the hybrid warfare at which they get their support quite often in a covert way from a state.
- Informational Activities: In hybrid warfare, manipulation and propaganda are the tools used in the media, and the aim is to influence masses in such a way that political objectives can be realized without direct military confrontation.

The theory of hybrid warfare in the context of India's strategy is an example of the interweaving of conventional and unconventional tactics through the media and proxy groups. Through this theory, the authors try to summarize the complex situation of hybrid warfare more understandably.

2.4.2 Security Dilemma Theory

Taking in mind the importance of the Security Dilemma Theory, it can be said that the theory perfectly explains the situation between Pakistan and its regional rivals, especially India. According to this theory, when one state increases its military power to ensure its security, neighboring states may see it as a threat, thus leading to them also building up their military capacity in return. This in turn leads to the arms race due to the fact that every country considers the others' acts aggressive, without a direct intention of ending pacify.

When the concept of hybrid warfare is taken into consideration, the security dilemma unfolds itself as in one state's defense so the other state interprets it as an offensive move such as military structural enlargement and cyber warfare endeavors. In such instances, the nation with the perceived enemy unleashes its hybrid warfare strategies of cyber warfare, disinformation, and other covert operations, targeting the stability of the presumed threat, thus without the use of open military conflicts. The ongoing disagreement between Pakistan and India over Kashmir and other border disputes is a key element in the concept of security dilemma where the two countries raise their military capabilities, leading to regional instability and opening the opportunity for hybrid warfare.

2.4.3 Constructivism and Narrative Warfare

International relations constructivism asserts that the social structures, identities, and narratives of a society are crucial factors in determining international behavior. The explanation is also helpful for elucidating the way of information warfare in South Asia. Constructivists hold the opinion that national security and war come from by reiterating one's identity, beliefs, and values.

Narrative Warfare is a subset of constructivism which implies the use of information warfare, propaganda, and the media to manipulate narratives and create meaning. Via narrative warfare, governments, terrorist groups, or other non-state actors are the regular players to manipulate the impression of the chosen audience as well as the entire international community. This process accomplishes several things simultaneously, including the change of the conversation to another set of meanings, the granting of legitimacy to the actions and finally, the denial of the adversary.

Narrative warfare is the area of hybrid warfare involving both India and Pakistan that has been the main instrument in media campaigns for local and international public opinion influence. With the help of social media, television, and other platforms, the creators and the broadcasters of these stories are playing an even bigger role in this narrative proliferation and in the attempt to counter the hybrid warfare.

Research Methodology

3.1 Research Design

The type of research design suitable for the present investigation is qualitative and descriptive in nature. The goal of the research is to unravel and scrutinize the existing strategies, vulnerabilities, and threats of hybrid warfare to Pakistan's national security. The research will be designed as a single case study to clarify the hybrid warfare through various dimensions such as the political, the military, the economic, and the cyber-related aspects, and will be a comprehensive study.

The design will be mostly about collecting past data such that it will provide usable data in the context of hybrid warfare in Pakistan mainly in terms of security challenges. The study will draw on various sources of information, e.g., direct sources ((government documents, policy papers, and security reports) and indirect sources (journals, books, and expert opinions) to present a balanced picture of hybrid warfare.

3.2 Data Collection Methods

The data will be collected using the following techniques:

Documentary Analysis: Government documents, security reports, policy papers, and white papers will be gone through to analyze the situation in the country regarding hybrid threats. One of the specific activities conducted will be the military and cyber space strategies and social-political frameworks that are in the country will be a subject of an overview.

Interviews with Experts: The researcher will use a semi-structured interview from the defense analysts, security experts, scholars, and government officials. These interviews will help the researcher to learn the implementation of the strategies against hybrid warfare and the identification of the defense and security system vulnerabilities in Pakistan.

Content Analysis of Media and Public Discourse: Examining media reports, opinion articles, and public discourse will be an effective approach to understand both the public's way of looking at hybrid warfare and the persons who come up with the issue and coverage. It also implies that there will be need to review social media platforms by media researchers to obtain the language of the misinformation campaign and how the campaign was executed in order to better understand the impact that the misinformation campaign has on national security.

Case Studies: Different cyber attacks, source incidents, or episodes which are the most typical hybrid warfare tactics used to give harm to Pakistan such as misinformation campaigns, and irregular military tactics will be analyzed one by one. This will definitely help those in charge to be able to plan meticulously a course of actions to curb the rampant biodiversity loss which leads to food security issues. Nevertheless, there might be people who would still get food through emerging and unconventional techniques.

3.3 Data Analysis Techniques

The obtained data will undergo the subsequent analysis techniques:

Thematic Analysis: This is the process through which themes and patterns are extracted and recognized, and at the same time the complexity of hybrid warfare strategies, vulnerabilities, and national security responses is studied. The qualitative data, derived from interviews and document reviews, interview data are the likely sources this method will be applied to.

Comparative Analysis: The study comparing several hybrid warfare strategies which were used in the case of Pakistan as well as other different countries can be cited as a comparative analysis. Hence, identification of the shared tactics, weaknesses, and ways of dealing with a breach is possible.

SWOT Analysis: The SWOT (Strengths, Weaknesses, Opportunities, Threats) is a widely used and popular analysis technique in assessing the internal and external conditions of an organization. The SWOT model can be used as a diagnostic tool to help analyze an enterprise's strengths, weaknesses, opportunities and threats for planning purposes, in decision making, and strategic thinking.

Descriptive Statistical Analysis: In case of the presence of quantitative data, descriptive statistics such as the frequency of cyberattacks, military incursions, or misinformation campaigns will be computed.

3.4 Limitations of the Methodology

Despite the comprehensive approach outlined above, several limitations may affect the research methodology:

Access to Sensitive Information: Access to classified or highly sensitive government and military information can be problematic giving the nature of the topic. This would leave fewer security strategies and vulnerabilities that the analysis of can be carried out.

Bias in Media and Expert Opinions: Reports from the media and expert opinions may be biased in their perspectives especially related to national security that is politically sensitive. To limit this bias the sources of data will be cross-referenced and checked by triangulation.

Limited Availability of Case Studies: Hybrid warfare that is still perplexing and changing, as well as the fact that the number of case studies particularly focusing on Pakistan will be few, can probably affect the quality of the strategic and tactical responses analysis to hybrid warfare.

Evolving Nature of Hybrid Warfare: It is in the nature of hybrid warfare strategies and tactics to be in a continuous evolving state and, most importantly, the time frame concerned with the collection of data may also limit the research.

Hybrid Warfare Strategies Against Pakistan

4.1 Military and Proxy Tactics

Hybrid warfare, simply defined, is nothing but a combination of regular war fighting and irregular warfare, including non-state actors, insurgents, and proxy forces. The case of Pakistan is a perfect example where proxy warfare is prevalent as a strategy by external actors to make a country unstable. Allegedly, the neighboring countries, especially India and Afghanistan, have been charged with using proxies to cut Pakistan's internal security and attack the country's sovereignty directly. One of the ways these groups,s such as Tehrik-i-Taliban Pakistan (TTP), Balochistan Liberation Army (BLA), and many other militants in Kashmir act is by being surrogates to the enemy, thus having insurgency and terrorist activities done within the territory of Pakistan.

Proxies play the game of warfare against Pakistan, primarily by sticking to the strategy of asymmetric warfare, the aim of which is to destroy or disable the enemy without offering direct opposition. It is all about very small forces with a profound ability to be creative in the military aspect. The adversaries are mostly the local militias who are backed by the regional state actors. Then, these specially trained soldiers conduct hits and a variety of tactics such as car bombs, etc., in various and multiple suicide attacks, targeted assassinations, and ambushes in the conflict-prone localities such as Balochistan, Khyber Pakhtunkhw,a and FATA. All these operations are simply executed to provoke a certain political and social crisis, and in addition, if realized, it would be much easier to get rid of the authorities who do not act accordingly.

Furthermore, besides financing them, these proxy groups are often arranged with military equipment by foreign powers. According to the reports, these powers have been shown to even promise to offer humanitarian assistance to the fighters for the aim of destabilizing the northern regions of Pakistan. This is where these powers are mediating the insurgent groups to reach their objectives strategically, politically or militarily.

The psychological aspect of proxy warfare has to be considered. Propaganda is a tool that these organizations use to manipulate the public, create hatred between people of different ethnic and religious backgrounds, and sow the seeds of distrust in the government's ability to keep the peace and ensure public safety.

4.2 Cyber Warfare and Technological Attacks

Cyber warfare in the recent times of hybrid warfare has assumed the role of a necessary and very important part of any conflict in the modern world. Cyberattacks make it possible for the enemy to attack a country's security without direct military intervention. In the case of Pakistan, hacking and cyber warfare are persistently high and have been used to attack and take over the country's critical infrastructure, acquire important information from the military, and issue fake information. Many of these acts were performed by a state's unit and referred to the wider context of that nation's use of power to deplete the military, the governmental systems and the economic system of Pakistan.

Cyber espionage has been one of the most successful strategies used, where criminals have stolen state secrets through access to government databases, the military and private companies' systems. Military and defense data are especially valuable to rivals, as it gives them intelligence and defense superiority in case a conflict would occur. Pakistan is regularly found to be on the receiving end of attacks that aim at interrupting military communications, stealing military secrets, and nuclear technology exposure.

One more vital area of cyber warfare is hindering communication systems. The opposition disturbs telephone, internet, computer, and other communication systems which could include power plants, banks, and grids, to cause extensive disturbances. Pakistan’s electricity grid was attacked in 2015, precipitating massive blackouts across the country. This may be a war that challenges Pakistan's infrastructure to cyberattacks and the lasting impacts on the national security of such incidents.

Information warfare is a highly essential aspect of cyber strategies. By means of social media, fake updates, and propaganda, the operators of cyber war can influence the views of people, create fears, and make sure that the leaders in Pakistan remain unbelievable. With the help of psychology, it is a kind of warfare that would create a lack of stability in a nation by raising mystification, breaking trust, and generating division in the society.

4.3 Economic and Financial Pressure Tactics

Apart from the military and cyber strategies, the pressure on the economy and the financial situation are tactics that are used to eliminate the power of a nation and bring about instability. In general, hybrid warfare encompasses financial strategies which are, for example, sanctions, embargoes, and other ways of financial control to put the national economy at risk. Mainly, Pakistan has been under considerable economic pressure that has been made even more difficult indeed by international sanctions and the restrictions of access to financial resources.

Financial sanctions are typically used as a weapon of economic warfare against Pakistan. As a result of the sanctions imposed by countries like the United States, or international bodies like the International Monetary Fund (IMF) and World Bank, Pakistan is restricted in global financial markets, foreign investment is blocked, and imports of energy resources and military equipment are prohibited. These sanctions also the side effect of reducing the country's financial stability, that is the ability to fund defense projects.

Also, the enemies of the country use the technique of currency manipulation to make Pakistan's economy grim. By reducing the value of the local currency through official exchange rates or transaction manipulation, external parties can provoke inflation, capital flight, and general economic turbulence in the country. This then forces common people to bear the burden financially and as a result, there will be protests which will weaken the social fabric of Pakistan.

Providing assistance to insurgent and separatist movements in challenging regions like Balochistan in Pakistan is another method of waging economic warfare. In a place like Balochistan, for instance, external forces may extend economic and logistical facilities toward insurgent groups. These militants' ultimate goal is to create chaos and thus they tend to disrupt the economy while the nation is divided and thus the growth potential is undermined. Adversaries can frustrate Pakistan's ability to counter hybrid warfare tactics by striking at its economic base.

4.4 Disinformation and Media Manipulation

Disinformation and media manipulation are the main tools of hybrid warfare. These tactics are used to create confusion, manipulate public opinion, and reduce societal stability by spreading untrue or misleading information. Hybrids have increasingly used disinformation campaigns to reach their goals in Pakistan.

1. Social Media and Digital Platforms: In this day and age, digital platforms have become the main battleground for disinformation. Social media platforms, like Facebook, Twitter, and WhatsApp, are often the grounds for the dissemination of disinformation and the incitement of violence, as well as the manipulation of public opinion. Apart from these, other statements are sometimes made. For example, fake news in the domain of political events, natural disasters,s or military operations can instill panic, destroy trust in the institutions of the government, and segregate society.

2. State-Sponsored Disinformation: In many cases, hybrid warfare takes the form of a conflict where state actors or proxy organizations use the media as tools to advance agendas that align with their interests. It is believed that in Pakistan the abovementioned foreign opponents have not only set up fake news organizations but also made use of the existing media to spread false or exaggerated stories. These stories are aimed at making the political situation unstable and the governance ineffective. Furthermore, online bots and fake accounts have been employed to increase disinformation levels and mislead people. This has] lead to foreign entities cementing misinformation and generating a false sense of security.

3. Disinformation has a devastating effect on national security: Besides the loss of public confidence in the state, it can be the trigger for the increase in the number of demonstrations that can even turn into civil unrest. In addition, a disinformation threat could divert security forces from the real danger, thus paving the way for the resources to be wasted in fighting what are false stories. At the same time, the disorder that the disinformation campaigns can create is likely to make the internal fissures more serious, and that will make Pakistan more susceptible to the external forces' intervention.

4.5. Psychological and Ideological Warfare

Warfare that comes under the psychological and ideological label of warfare is aimed at influencing and manipulating the perceptions, beliefs, and attitudes of individuals or groups in the target population. The main goal of this kind of warfare is the disarming of the enemy, the creation of discord, and the cultivation of internal divisions, all of which would then make the nation more responsive to external influence.

1. Exploiting Religious and Ethnic Divides: The enemies of Pakistan always resorted to religious and ethnic differences to achieve their goal of inciting unrest in the country. The role played by foreigners in spreading extremist ideologies can not only lead to violence but also cause fear and suspicion among disparate groups. This is how society becomes segmented into groups with different values, and thus, national unity is compromised, which may, in turn, obstruct the solution of hybrid threats.

2. Radicalization and Recruitment: Psychological methods are another tool used in hybrid warfare to lure people into insurgent or terrorist organizations. Vulnerable parts of society are affected by extremist ideologies that are spread through the internet, and the messages can have a very powerful impact on these people and cause them to be recruited. For example, the local online propaganda can cloud the minds of the younger segments of the society, which can result in the young people being involved in insurgent activities and therefore destabilize their state.

3. Use of Propaganda in Conflict Zones: The psychological war in areas prone to conflict, such as those near the Afghanistan border, is manipulative and is directed towards the local population to revolt against the government. The main objectives of the propaganda campaigns are to cultivate a feeling of being a victim, increase the associated insurgent groups' support, and diminish the public trust in the security forces. The efficiency of such propaganda is made even more potent by the citizens' grievances, whether it is governance, ethnic identity, or economic disparity related.

4. Erosion of National Morale: Right from the very beginning, psychological warfare includes the destruction of people's national pride. By tampering with the media, the opposition can spread the notion of Pakistan being either a divided or a feeble country, leading to internal frustration. The psychological operations are also capable of demeaning the armed forces by, for example, carrying out propaganda that cuts the ground from under them or depicts them as ineffective in responding to hybrid warfare

These strategies are just a few examples of the hybrid warfare tactics used against Pakistan’s national security. The fusion of traditional military operations with non-traditional tactics like disinformation and psychological warfare complicates the country's defense strategy and requires a multi-faceted response from the government and its institutions.

Pakistan’s Vulnerabilities and National Response

5.1 Political and Institutional Vulnerabilities

Hybrid warfare is practiced for the purpose of taking a nation's internal political weaknesses and Pakistan is used as an example of that. The country experiences shaky political situations marked by fast-changing governments, little political agreement, and a decline in public institutions. Such factors limit the state's possibilities to come up with security and defense policies that remain unchangeably in place for a long time and control tactical changes in the development. The politics in the country are mostly in a scenario with the ruling party not being only outright enemies of their political rivals but also have members within their rank who oppose them. This makes the process of decision-making slow and encourages external actors more to penetrate the country’s social fabric.

The combination of corruption and poor government performance has been the situation’s problem. The well-anchored and institutionalized corruption, especially in government organizations, give birth to inefficiencies that can sabotage Pakistan’s national security agenda i.e. securing borders, dealing with internal security issues, and even the development of the nation in the long run. Furthermore, the rising political polarization among the leading political parties has led to a division, which has resulted in a situation that is easily exploitable in hybrid warfare scenarios. The differences among the population make it less resistant and more likely to change, thus leading to efforts to destabilize the nation from its leaders as well as external forces.

5.2 Cybersecurity and Technological Gaps

The upsurge of digital warfare has changed the game by making cybersecurity an essential feature in hybrid warfare strategies. The lack of a cybersecurity infrastructure in Pakistan is the reason the country is greatly exposed to cyber-attacks that target the country’s critical areas such as energy, defense, and finance. A big concern is also the fact that the country does not have a robust, unified national cybersecurity framework that can effectively react to the development of the threat landscape. Moreover, the fact that Pakistan is dependent on foreign countries for both hardware and software solutions makes it more vulnerable. These international dependences pave the way for Pakistan to be a victim of espionage, cyber-espionage, and technological resources being destroyed. Further, Pakistan's very limited technological resources and not enough of a cybersecurity education in institutions exacerbate the issue. The educational sector and research programs in the field of cybersecurity in the country are not strong, leading to the lacking of professional staff who can counter the increasingly intelligent cyber threats. This technological inadequacy hinders Pakistan in its fight to protect its sovereignty from the technologically advanced modern warfare tactics. In conclusion, the digital divide among parts of Pakistan says that some parts are at a higher level of risk for cyber manipulation, with not much access to the required tools for defense.

5.3 Economic Fragility and External Dependencies

Economic vulnerabilities are a crucial element in hybrid warfare, and Pakistan’s economic weakness makes it vulnerable to various forms of interference from outside. Pakistan’s economy has had to put up with chronic problems such as hyperinflation, high public debt, not enough industrial production, and an over-dependence on agriculture. These bottlenecks solarize the country to external economic influences such as a ban on trading, foreign sanctions, and market manipulation. The latter of the two triggers an additional challenge as the money inflow into the country from other countries particularly the IMF, only worsens the already high problem of vulnerability. The resource that can one day be a key for Pakistan's economic revival is now available for use by the outside forces seeking to bring about a new economic order, especially in the context of economic hardships.

What's more, the dependence of Pakistan on the importation of oil and gas, especially the former, makes it an easy target for possible global energy market disruptions that can be manipulated as a weapon in hybrid warfare situations. An example of the same is that if there would be an overnight increase in global energy prices, or an oil supply chain was cut, the impact on the Pakistani economy would be catastrophic. Subsequently, the country is suffering from grave issues in the sphere of human development with the education, healthcare, and social service areas witnessing the most substantial deficiencies, therefore, leading to a deficiency in the skilled workforce that the country can potentially produce. Thus, the waning of the human capital available for the country’s defense against hybrid warfare begins to appear as the most fundamental bottleneck straining up the overall progress of the country.

Table: Key Vulnerabilities in Pakistan’s National Security

Category	**Vulnerabilities**	**Implications for Hybrid Warfare**
Political and Institutional	- Political instability	- Fragmented decision-making, weakened governance, vulnerability to internal political manipulation
	- Corruption and weak institutions	- Inefficiency in national security policies, weakening of state response capabilities
	- Political polarization	- Easy exploitation of internal divisions by external actors

Cybersecurity and Technological	- Lack of a centralized cybersecurity framework	- Increased susceptibility to cyber-attacks targeting critical infrastructure (e.g., power grids, financial systems)
	- Technological dependence on foreign nations	- Potential espionage, sabotage, and control over key technological resources
	- Digital divide and lack of skilled professionals	- Greater vulnerability in rural areas and reduced national ability to defend against cyber threats
Economic Fragility	- Economic instability (inflation, public debt)	- Greater susceptibility to economic coercion, trade embargoes, and the destabilizing impact of economic warfare
	- External dependencies (foreign aid, energy imports)	- Economic leverage exerted by foreign powers, reliance on external support for stability
	- Human development deficits (education, healthcare)	- Reduced resilience to hybrid warfare tactics that target the societal and economic foundations of the state

5.4 Media Control and Public Narrative Weaknesses

Control of media and public narrative is an important tool in countering hybrid warfare, which is gaining more and more significance. In this case, Pakistan's media is decisive in the formation of the public perception about national security threats, especially the threat of the hybrid warfare, which, like in this case, combines conventional military actions with information warfare, cyber-attacks, and social media manipulation. The manipulation of the media by external actors is Pakistan's biggest vulnerability, and these actors spread disinformation, propaganda, and false narratives by the openness of the internet and media in the country. Hybrid warfare, which is inclusive of the psychological war, is basically about exploiting the information to weaken authorities, cause friction inside society, and direct the public opinion. Besides using traditional media channels, enemies, both of the state and other actors, have also taken advantage of digital platforms to fuel sectarian divisions, political unrest, and social instability in Pakistan (Akhtar & Khan, 2019).

Moreover, Pakistan has a disintegrated media landscape, where the different media outlets are under the control of various political and ideological factions. This division impairs the formation of a national narrative leading to a state response that is susceptible to weakness against hybrid warfare strategies. Different media outlets supply different versions of events, which when presented to the audience at the same time arouses confusion and shatters the respect that people have for state institutions. This situation, in fact, is more severe in the case of hybrid threats. The government’s lack of proper media strategies makes the process of confronting the external manipulation of information less rigorous than it would otherwise be

(Hussain, 2021). In the event of a hybrid war, not only do social media platforms facilitate the spread of true information, but they also become the main targets for the intended distribution of misguiding information. The infiltration of those platforms by extremists, the spread of fake news, or the calls for violent demonstrations through these platforms have emerged as very serious problems that obstruct Pakistan's efficient media regulation (Farooq, 2020).

In such a way, the measures employed by the government to bring order to the media are seen in the form of policies adopted to combat the fake news and misinformation menace, but so far, the battle has not resulted in any positive outcomes as these measures are very local. This oversight is the fault of a permanent lack of consistency in the media regulations that is sometimes shadowed by political parties, and this compromise of media independence from government intervention makes the regulation process even more challenging (Zaidi, 2021). Pakistan as a country that has been subjected to hybrid war for a long period is directly associated with the lack of efficient media regulation, which leaves both the media and the country as a whole vulnerable to attacks with the external factor supplying the malevolent forces (Zaidi, 2021).

5.5 Exploring The Employed Strategies and Their Downfalls

Pakistan's present strategies to counter hybrid warfare involve military actions, cybersecurity to keep attackers out, sharing intel with allies, and national security measures orientated towards the removal of the menace of terrorism and fanaticism. However, these strategies do not always fully address the multifaceted nature of hybrid warfare. The military has been the leading force in Pakistan's defense against not only conventional threats but also hybrid warfare. Although the military has made progress in cyber defense and counterterrorism operations, hybrid warfare has not been effectively dealt with as a result of narrow-down strategy. Pakistan's over-reliance on traditional military forces and the fact that they are busy with other operations like internal security prevent it from being swift in responding to the broad range of tactics deployed in hybrid warfare (Khan, 2018).

Cybersecurity and digital defense have been put forward as vital areas for Pakistan's hybrid warfare strategy. Some measures like the establishment of the National Cyber Security Policy and the introduction of institutions such as the National Response Centre for Cyber Crimes (NR3C) breathe hope, however, Pakistan, which is under evaluation, is still behind the rest of the world in cyber defense. The money and staff Pakistan dedicates to counter cybercrimes are not enough and even what is available is disorganized and ill-equipped to take on the threats effectively (Farooq, 2020).

Moreover, the reliance on reactive rather than proactive strategies, such as addressing cyber incidents only after they occur, leaves Pakistan vulnerable to cyberattacks that can cripple national infrastructure or disrupt communications in the event of a hybrid warfare campaign. Collaborating with the United States and China amongst others in intelligence gathering and sharing is a key element in Pakistan's fight against hybrid warfare. Decision-makers of intelligence organizations are of great help in finding new threats and preventing or reducing hybrid attacks. Generally, the performance of these relationships is often hampered by the impact of political choice, mistrust among partners, and red-tape. In addition to this, the intelligence services in Pakistan are not yet fully integrated which makes the sharing of timely crucial information between them difficult. On the other hand, the sharing of vital data is a prerequisite for emergency response to the hybrid threats and a major missing factor in the intelligence.")

The third link of the Pakistani hybrid warfare strategy - not having a joint strategic communication framework - is the most striking. Pakistan so far has built solid infrastructure for defense and intelligence, but it has no comprehensive strategy to be able to effectively respond to disinformation and fake news weapons. The country’s steps for online public disinformation, sham, and external manipulation are not proactive, but they are rather reactive, fragmented, and often incomplete. Pakistan’s inability to establish a national narrative brake to set expectations allows third parties to exploit the information gap further while worsening societal and political divisions (Hussain, 2021). Devoid of an effective communication strategy, hybrid warfare adversaries have full potential to shape public opinion, meddle with political affairs, and eventually cause chaos and confusion in the country.

Finally, political instability, corruption, and a lack of cohesion between civilian and military leadership contribute to Pakistan’s vulnerability in hybrid warfare. The country’s political landscape is marked by significant polarization, which is often exacerbated by corruption, making it difficult for the government to maintain effective governance and respond swiftly to hybrid threats. Social divisions, driven by factors such as sectarianism and ethnic tensions, provide ample opportunities for external actors to exploit weaknesses within society and deepen divisions (Zaidi, 2021). The absence of a cohesive national response, both politically and socially, severely limits Pakistan’s ability to mitigate the effects of hybrid warfare.

Conclusion

The report on "Strategies and Vulnerabilities to Hybrid Warfare Against Pakistan's National Security" confirms that hybrid warfare is a multilayered threat, which includes regular, irregular, and cyber tactics to access political, strategic, and military goals. The section has suggested measures to be taken and gives the summary of all chapters, the main issues resolved, options for the future work and specific measures to be taken in the area of ensuring the National Security of Pakistan from the threat of hybrid warfare. Hybrid warfare also has many features and is a moving target with new dynamic threats. However, through the understanding of the same and the opening of loopholes, Pakistan can move to prevent these threats actively.

Key Findings

The Identification of hybrid warfare strategies implemented against Pakistan shows:

Twofold Character of Hybrid Warfare: It is the fact that hybrid warfare is a combination of processes and non-process actions, such as military aggression, economic destabilization, cyber-attacks, disinformation campaigns, and proxy warfare. These methods are supposed to directly take advantage of the targeted state's weaknesses directly, be they political, military, or social systems

Vulnerabilities in National Security: The weaknesses in the way Pakistan is governed, unrest in political circles, economic troubles, easily accessible borders, and the insufficient cyber security problem are the main reasons why the country can be open to hybrid warfare attacks.

Role of External Actors: The intervention of both state and non-state agents in hybrid warfare against Pakistan interfaces with the ambiguous geopolitical situation in the region. Individuals/Entities that are interested in gaining an edge by weakening Pakistan undertake hybrid warfare to reach some of their objectives, such as getting the land they want, spreading their faith, and establishing the zone under their domination.

Cyber and Information Warfare: Cyber-attacks and the spread of misinformation have turned into the core factors of hybrid warfare. Pakistan's vital national security information has been undermined by adversaries who have used cyber espionage, inserted malware, and run propaganda in a coordinated way.

Impact on Socio-Political Stability: Hybrid warfare tries to destroy the confidence the populace have in government bodies and make rifts between various groups. The well-thought-out manipulation of mass media and social networks to influence people's opinions has remained an effective method for causing turmoil in the socio-political situation of the country.

Recommendations

Based on the findings, the following suggestions are made to fight the impact of hybrid warfare and to improve the national security of Pakistan:

Strengthening Governance and Political Stability: Pakistan's strategy in countering hybrid threats should revolve around the issue of mitigating political instability, improving governance, data transparency, and the democratic character of politics. Efficient and transparent leadership will be the cornerstone that will allow remaining vulnerabilities to be removed. (adapted from original due to context)

Enhancing Cyber Security and Digital Infrastructure: By doing so, Pakistan will not only protect its cyber system through the purchase of the most advanced technologies but will also create a cyber police force that will be responsible for the security of critical infrastructures. Moreover, the awareness of online threats among the general public and decision-makers is critical for both the officials and the country itself to recognize and remove, or at least diminish the severity of such threats. (paraphrased from source)

Improving Economic Resilience: The efforts to strengthen the economy of the country are an indispensable condition for it to be capable of pursuing the hybrid warfare in a secure manner that is not conducive to the influence of money from the outside; Undeniably, financial diversification is key to the health of the economy, fiscal discipline is the engine that should be used to achieve financial; independence, and functional aid justification is the first step. by which the country will lose money. That is less than the loss that the enemy would get after it hears about your capability.

Fostering Regional Cooperation: Establishing strong relations with not only neighbors but also international governmental and nongovernmental organizations can be the force that acts in the same direction, defending the states from and multinational organizations can be enlisted to form a united front in the battle against the hybrid warfare. Among the methods are intergovernmental security agreements, intelligence swapping, and cooperation in defense projects which will aid Pakistan in confronting hybrid threats better.

Countering Disinformation and Propaganda: Pakistan must develop a robust strategy to counter disinformation campaigns. This includes improving media literacy, establishing a fact-checking framework, and enhancing the role of state-owned media in promoting accurate narratives.

Developing Hybrid Warfare Counter-Strategies: Pakistan should invest in research and development of hybrid warfare counter-strategies, including asymmetric warfare tactics, psychological operations, and intelligence capabilities to preemptively identify and neutralize hybrid threats

References

Clarke, R. A., &Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.

Hoffman, F. G. (2007). Hybrid Warfare and Challenges. The Marine Corps Gazette.

Buzan, B., Waever, O., & de Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner Publishers.

Mearsheimer, J. J. (2001). The Tragedy of Great Power Politics. W.W. Norton & Company.

Barnett, M. (2008). Culture, Structure, and History: A Comparative Analysis of National Security Systems. International Security, 22(2).

Cavelty, M. D. (2007). Cyber-Security and the Politics of Risk. The International Journal of Communication, 1, 144-168.

Akhtar, M., & Khan, M. (2019). Hybrid Warfare and Its Impact on National Security: The Case of Pakistan. Journal of International Security Studies, 22(1), 45-58.

Farooq, M. (2020). Cybersecurity and Hybrid Warfare: Pakistan’s Vulnerability. Asian Journal of Security Studies, 18(3), 123-137.

Hussain, M. (2021). The Role of Media in Hybrid Warfare: Pakistan’s Strategic Vulnerabilities. South Asian Journal of Media Studies, 11(2), 34-49.

Khan, S. (2018). Hybrid Warfare and the Information Age: Pakistan’s Response to Emerging Threats. Pakistan Defence Review, 29(4), 90-104.

Rehman, F. (2022). Strategic Communication and the Fight Against Hybrid Warfare in Pakistan. Global Security Review, 14(1), 75-88.

Zaidi, A. (2021). Political Instability and Hybrid Warfare in South Asia. South Asian Politics and Security Journal, 13(3), 122-137.

Waltz, K. (1979). Theory of International Politics. Addison-Wesley.

Cordesman, A. H. (2019). China and the Evolving Military Balance in the Asia-Pacific: Strategic and Budgetary Trends. Center for Strategic and International Studies (CSIS).

Galeotti, M. (2016). Hybrid War or GibridnayaVoina? Getting Russia's non-linear military challenge right. Mayak Intelligence.

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

Norrlof, Carla. "Economic Statecraft in the Age of Sanctions." Cambridge University Press, 2016.

Baldwin, David A. "Economic Statecraft." Princeton University Press, 1985.

Mearsheimer, John J. "The Tragedy of Great Power Politics." W.W. Norton & Company, 2001.

Katzman, Kenneth. "Pakistan: Terrorism, Security, and the Cost of War." Congressional Research Service, 2010.

Mowatt-Larssen, R. (2010). Psychological Operations: A Weapon of War in the Age of Information Warfare. Stanford University Press.

Hassan, A., &Shaukat, F. (2020). The Role of Ideological Warfare in Hybrid Conflicts: Case Studies from South Asia. Asian Security, 41(1), 56-74.

Clarke, Richard A., and Robert K. Knake. "Cyber War: The Next Threat to National Security and What to Do About It." Ecco, 2010.

Schmitt, Michael N. "The Law of Cyber Warfare." Oxford University Press, 2013.

Kilcullen, D. (2009). The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One. Oxford University Press.

Marten, K. (2015). Russia’s Use of Semi-State Security Forces: The Case of the Wagner Group. Post-Soviet Affairs, 31(4).

NATO (2010). Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.

NATO (2015). Countering Hybrid Warfare. NATO Parliamentary Assembly.

Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.

Khan, Z. (2020). "India’s Hybrid Warfare Against Pakistan: An Analysis." Journal of Security Studies, 12(1), 45–67.

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

Renz, B., & Smith, H. (2016). "Russia and Hybrid Warfare – Going Beyond the Label." Aleksanteri Papers, 1, 1–40.

NATO. (2015). "Hybrid Warfare: A Challenge to Adapt." NATO Review Magazine.

Ahmed, Z. S. (2017). Security Challenges to Pakistan: Hybrid Warfare and the Need for Strategic Foresight. South Asian Journal of International Affairs.

Giles, K. (2016). Handbook of Russian Information Warfare. NATO Defense College.

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

Kofman, M., &Rojansky, M. (2015). A Closer Look at Russia's "Hybrid War". Wilson Center.

Mansoor, P. R. (2012). Hybrid Warfare in History and Theory. In Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge University Press.

NATO. (2019). NATO's Response to Hybrid Threats. Retrieved from https://www.nato.int