



Journal of Emerging Trends in Social Sciences and Humanities

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

E-ISSN: [3006-7898](#) P-ISSN: [3006-788X](#)

Volume 3, Issue 2, 2026, 133-143



Hybrid Warfare and Pakistan's National Security: Assessing Emerging Threats and Building National Resilience

Irteza Shabbir¹ Dr. Adeel Irfan²

¹ Research Scholar, Department of Political Science, University of Sargodha, Punjab, Pakistan.

² Master Trainer, CVE, Assistant Professor, Department of Political Science, University of Sargodha, Punjab, Pakistan.

Corresponding Author: Dr. Adeel Irfan, Email: adeel.rao@hotmail.com

Article Information

ABSTRACT

Received:

2026-04-13

Revised:

2026-05-14

Accepted:

2026-06-16

Keywords

Hybrid Warfare; Pakistan's National Security; National Resilience; Gray-zone Conflict; Cyber Warfare; Information Warfare; Regional Security Complex; Stability–instability Paradox.

Hybrid warfare has become one of the biggest threats to modern-day national security, especially for countries that have complex regional security contexts. Hybrid warfare is the use of military and non-military measures (such as cyber-attacks, information warfare, economic pressure, proxy conflict, law warfare, psychological warfare, etc. Located in a strategically critical South Asian environment, Pakistan is grappling with a growing array of hybrid threats to its national security, institutional efficiency and strategic independence. This study explores the changing dynamics of "hybrid warfare" and analyzes its implications for Pakistan's national security by analysing the threats in the political, military, cyber, economic, informational and diplomatic fields. The study adopts a qualitative research design using descriptive and analytical approaches and secondary data are collected through scholarly literature, policy documents and official reports. The analysis is based on the Stability – Instability Paradox and Regional Security Complex Theory to explain the South Asian dynamics of hybrid conflict in addition to the strategic environment that Pakistan operates in. The study concludes that preparedness for conventional military action is not enough to tackle the multidimensional aspect of hybrid warfare. Rather, the building of national resilience via effective civil-military coordination, institutional capacity, cyber security, strategic communication, economic stability and societal cohesion is a precondition to deal with the changing nature of hybrid threats. Finally the paper suggests an integrated national resilience framework to improve Pakistan's readiness for facing present day hybrid threats and protect its national security interests in the future.

1. Introduction

Warfare in the 21st century has taken a radical turn

from conventional warfare to multidimensional warfare using a combination of military and non-military methods. Today's conflicts have been



© 2026 by the authors. Licensee Shabbir & Irfan. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license <https://creativecommons.org/licenses/by/4.0/>

Publisher: Institute for Educating Environmental Resilience and Governance

accompanied by cyber operations, information warfare, economic coercion, proxy actors, diplomatic pressure, psychological operations, and strategic communication to meet political and strategic goals without entering into a full conflict. What can be called hybrid warfare represents a new type of conflict that brings the concept of national security beyond the traditional military prism to the political, economic, technical, informational and societal sphere (Huşanu, 2026).

The effectiveness of hybrid warfare has been considerably improved by the rapid development of technology, globalisation, digital connectivity and the universalisation of social media. Cyberspace, artificial intelligence, disinformation, economic influence and cognitive operations are increasingly used by both state and non-state actors to influence public opinion, erode state institutions and impact strategic decision-making. Therefore, the challenges facing security today are not limited to military threats as they now have a wide range of multidimensional and interconnected threats that demand multidimensional and comprehensive responses (Hatim, 2025).

The strategic landscape of south Asia is extremely precarious and the region is known for its historical rivalries, unresolved territorial disputes, nuclear deterrence, cross-border terrorism, and ongoing geopolitical competition. In this intricate strategic landscape, the competition between Pakistan and India has now become more of a grey zone affair, where other means of power are used to attain strategic ends without resorting to full-scale conventional military conflicts. This shift has turned hybrid warfare into a key aspect of the regional security landscape (Radzi, 2026).

Pakistan is a geopolitically important country, lying at the intersection of South Asia, Central Asia, the Middle East, and the Indian Ocean. With the country's geostrategic significance, coupled with the changing security dynamics in the region, different forms of hybrid threats have emerged. The country is facing various hybrid threats such as cyberattacks, disinformation campaigns, proxy violence and economic coercion, diplomatic pressure, and attempts to exploit the country's political, ethnic, and sectarian divisions. The multidimensional threats not only pose a threat to Pakistan's defence

preparedness but also pose threats to the governance, institutional credibility, economic stability and social cohesion, and thus, are more than military threats (Kausar, 2026).

The nature of conflict is shifting, and military means are not enough to resolve hybrid warfare challenges. The contemporary national security should be not only based on the military readiness but also on the effective governance, cyber security, institutional resilience, economic stability, strategic communication, intelligence coordination and public confidence. In this context, the concept of national resilience has become an integral part of security policy, reflecting the capacity of a state to prepare for, withstand, adapt to and recover from multidimensional threats and ensure governance and societal stability (Naseeb, 2026).

Despite a growing body of academic literature on hybrid warfare in recent years, most of the current literature focuses on conceptual debate, cyber operations, or information warfare in isolation, or on strategic competition in a region. There is comparatively lesser literature that has taken a comprehensive look at the impact of the evolving hybrid threats on national security of Pakistan, and explored national resilience as a long-term strategy to counter the threats. This divide presents the need to link hybrid warfare with political, economic, military, cyber, information and societal security of Pakistan (Lal, 2025).

In this perspective, the present study reviews the shift of Hybrid warfare and their implications for the security of Pakistan by identifying the key hybrid threats of the country and analysing their strategic impact on various domains. Moreover, the study recommends a robust national framework to build Pakistan's resilience in long-term security in a complex strategic environment, which includes institutional capacity, cyber preparedness, strategic communication, civil-military coordination, economic resilience, and societal cohesion as the vital components of the framework (Ali, 2026).

2. Literature Review

2.1 Conceptual Evolution of Hybrid Warfare

The term 'hybrid warfare' has undergone substantial development in adaptation to the new realities of today's warfare. At first, the concept of

warfare was considered as a traditional battle between sovereign states; but in the era of globalization, technological development, and the rise of non-state actors, the face of security has changed. The modern conflict is more often characterized by a combination of traditional and non-traditional tools: cyber tools, information warfare, economic pressure, proxy forces, legal tools and psychological pressure. Such a multidimensional strategy allows opponents to pursue their goals without escalating to the level of a formal declaration of war, making it difficult to respond to them in the traditional way of a security approach (Huşanu, 2026).

Academic writing on hybrid warfare has taken on new meanings, not just in the field of military affairs, but also in the fields of politics, economics, information, technology, and society. Recent scholarship suggests that hybrid warfare cannot simply be understood as a tactics on the battlefield, but as a whole strategy used to act on the opponent's vulnerabilities and soft spots, in order to impact political decision-making processes, lower the legitimacy of the institutions and challenge the social cohesion. The use of digital technologies, artificial intelligence, cyber capabilities, and strategic communication have further improved the effectiveness and adaptability of hybrid strategies in the current international politics (Hatim, 2025).

Another major contribution in the literature is the understanding that the effectiveness of hybrid warfare is much more dependent on the vulnerabilities of the target than on the target's military strength. The lack of governance, polarization, economic instability, cyber insecurity, ethnic divisions, and erosion of public trust provide opportunities for external groups to wield intrusive influence over domestic affairs without the need for overt military action. Therefore, there is a strong need to build national resilience in addressing hybrid threats, which cannot be overstated (Kausar, 2026).

The literature also underscores that hybrid warfare is a feature of twenty-first century strategic competition as a way for the actors of conflict to achieve geopolitical goals through ambiguity, deniability, and the gradual escalation. Conventional warfare has a war-winning objective, but hybrid warfare is a strategy that

aims to drive a change in the strategic behaviour of other countries in order to achieve this through a combination of military pressure, political influence, economic leverage, cyber activities, diplomatic efforts and information manipulation. The development is a paradigm shift in the nature of the conflict and the need for all-inclusive national security policies to deal with multidimensional threats (Radzi, 2026).

2.3 Hybrid Warfare in South Asia: An Evolving Security Challenge

From the past two decades, the strategic situation of this region has changed drastically due to continuous geo-political tensions, nuclear deterrence, territorial issues, technological advancement, and the rise of non-conventional security threats. Strategic competition is no longer limited to conventional military competition but has also spilled over to the cyber realm, information arena, economic tools, diplomacy, and proxy networks. The changes have changed the security landscape in the region and have made hybrid warfare an effective tool of statecraft. (Azad, Haider, & Sadiq, 2023).

One of the most telling cases of the embedding of hybrid warfare in the modern regional security competition is the Pakistan–India rivalry. The strategic costs of direct conventional military confrontation have risen significantly with both states having credible nuclear arms. As a result, the area of competition has increasingly expanded to the “gray zone” – with cyber operations, strategic communication, disinformation campaigns, diplomatic pressure, proxy violence, economic influence, and legal instruments. These methods allow for states to achieve their political and strategic goals, without the risks of escalation that come with traditional warfare. (Bankov, 2024).

Current discussions on hybrid warfare in South Asia also emphasize that such a definition should not be exclusively related to military aspects. Rather, it is an all-in-one approach including political maneuvering, technical abilities, economic power, information control and mental manipulation to influence public opinion and to reduce institutional capacity. The recent research on modern conflicts, especially the Russia-Ukraine conflict, has shown that a successful hybrid campaign requires the coordinated use of

military and non-military instruments in various domains and this has important lessons for emerging security challenges in South Asia. (Iskandarov & Aliyev, 2026).

The shift in focus to hybrid threats has also resulted in a new focus on national resilience in the academic world. More than just military readiness, recent studies have emphasized the need for resilient political institutions, more sophisticated capabilities in cyber, cyber-ready critical infrastructure, strategic communication, economic stability and informed societies that are not easily manipulated by external actors to respond to hybrid warfare. National resilience, therefore, has become an integral part of the national security policies of each country, especially those in a complicated security landscape like South Asia. (Bjørge & Høiby, 2024).

2.4 National Resilience as a Contemporary Security Paradigm

The escalating complexity of hybrid warfare has greatly influenced the current national security discourse and hence shifted the focus towards national resilience as the cornerstone of the modern defense strategy. National resilience is more than just military strength – it is the ability of a country to prepare for, resist, adapt to and recover from multi-dimensional threats as it continues to operate, maintain economic stability and social cohesion. More recent research suggests that resilient states are better able to withstand external interference as they have more robust institutions, effective crisis-management processes, and higher levels of trust in state structures (Bjørge & Høiby 2024).

There is also literature that would suggest that national resilience extends beyond military preparedness to include political stability, economic sustainability, cyber security, strategic communication, protection of critical infrastructure, intelligence coordination, and society awareness. Hybrid threats typically look for institutional weaknesses, political polarisation, economic fragilities and information disorder alongside kinetic military force. As a result, resilience across these interrelated areas has now emerged as a fundamental necessity to securing the national sovereignty and future security in today's increasingly volatile international

landscape (NATO, 2023).

Recent research also calls for the need to take a whole-of-government and whole-of-society approach to effectively respond to hybrid threats. This will foster collaboration between the government bodies, military, intelligence services, academia, the private sector, media and civil society to build the national capability to respond to future security threats. This integrated approach to national security acknowledges the need for a combined institutional response that is capable of responding to the external and internal dimensions of hybrid conflict (OECD, 2022).

2.5 Research Gap

The current body of literature has significantly contributed to the academic study of hybrid warfare, but some gaps still need to be addressed. Researchers study the individual aspects of hybrid conflict, like cyber warfare, information operations, proxy warfare or strategic communication, but do not connect them in an all-encompassing national security framework. Similarly, the research available is mostly based on the European or Middle Eastern security context, with relatively little research exploring the specific nature of hybrid warfare in South Asia and its implications for Pakistan's national security (Lal, 2025).

Moreover, research on hybrid threats has often focused mainly on military and/or strategic aspects, neglecting governance, institutional resilience, economic security, societal cohesion, and policy coordination to a lesser degree. For this reason, a multi-dimensional analytical framework for Pakistan that assesses the impact of hybrid warfare on Pakistan's political, military, cyber, economic, diplomatic, informational, and social facets still exist. This is crucial to fill the vacuum for creating evidence-based policy responses that can enhance the resilience of Pakistan against emerging Hybrid Threats (Ali, 2026).

Accordingly, this study aims at filling these gaps by offering a comprehensive national resilience framework which will integrate security, governance, institutional capacity, cyber preparedness, strategic communication and societal resilience under a single analytical lens and by offering an integrated assessment for emerging hybrid threats facing Pakistan. The

study not only adds to the theoretical and policy-based literature on hybrid warfare, but it also provides practical suggestions for enhancing the national security of Pakistan, particularly in the long run (Huşanu, 2026).

3. Theoretical Framework

The principal analytical framework of this study are Stability–Instability Paradox and Regional Security Complex Theory (RSCT), which are used to investigate the changing nature of Hybrid warfare and its implications on Pakistan's national security. These theories are supported by the concept of National Resilience, which offers a holistic view of the way in which states are capable of responding to multidimensional security threats. These theoretical frameworks enable a holistic view of the strategic dynamics in South Asia and shed light on why hybrid warfare is increasingly being adopted as a means of competition between states (Khan, 2023).

3.1 Stability–Instability Paradox

The Stability–Instability Paradox is a concept that describes how at the nuclear level, strategic stability could promote strategic instability at lower levels of conflict. Pakistan and India have credible nuclear deterrence and the chances of a full-scale conventional war are reduced significantly. This strategic stability, however, has made both state and non-state actors use indirect means to achieve political goals without nuclear escalation like cyber-attacks, proxy warfare, information campaigns, economic coercion, and diplomatic pressure. In this context, hybrid warfare becomes a preferred option for engaging an adversary without the risks of conventional warfare, thereby becoming a key approach in the Russian foreign policy. Hybrid warfare is thus becoming a key tool in the Russian foreign policy, since it is less risky than conventional warfare and is more effective in influencing an adversary. The fight was a traditional military one (Krepon, 2020).

In the Pakistan–India framework, the Stability–Instability Paradox is a valuable explanation of why grey zone competition has been gaining ground. With the advent of nuclear deterrence, direct military confrontation has been limited, but competition has been possible, albeit it is conducted in non-kinetic and sub-conventional

forms. Such a theoretical approach can therefore be used to account for the fact that hybrid warfare is not a short-lived security issue but a constant phenomenon in the strategic interactions of the region (Narang, 2021).

3.2 Regional Security Complex Theory (RSCT)

Barry Buzan and Ole Wæver have developed a theory of regional security, which states that security threats are largely regional as the security of neighbouring states are closely linked. In this view, the security perceptions and policy responses of one state are affected by the actions of another state, and that is an inevitable part of being in a regional security complex. As one of the world's major security complexes, South Asia has a long history of interstate rivalry and rivalry within the region, unresolved territorial claims, nuclear deterrence and cross-border terrorism, alongside geopolitical competition (Buzan & Wæver, 2003).

Hybrid warfare should be considered from the perspective of regional strategic competition, not as a stand-alone security issue, as seen from RSCT. Political crises, information campaigns, cyber incidents, proxy conflicts and diplomatic confrontations often have regional security implications and cross borders. Hence, it is important to study hybrid warfare in the context of a regional security landscape to gain a complete picture of the current security challenges and responses in Pakistan (Ahmed, 2024).

3.3 National Resilience Framework

The concept of National Resilience offers a policy-oriented tool for coping with hybrid warfare in the context of multidimensional threats, as the Strategic Roots for the Stability–Instability Paradox and RSCT outlines the strategic genesis and regional dynamics of hybrid warfare. National resilience is the capacity of state institutions and society to anticipate, absorb, adapt, and recover from internal and external shocks and stresses while maintaining governance, unity and strategic goals. With the rise of hybrid threats, resilience has become a key part of a nation's ability to withstand and withstand security challenges, a consideration increasingly reflected in contemporary security literature, which regards resilience as an indispensable part of national security, as its main focus is on vulnerabilities in

institutions, trust, economy and society rather than on military force alone (Bjørge & Høiby, 2024).

Building national resilience in Pakistan will need an all-encompassing approach which will involve effective governance, institutional coordination, cyber security, strategic communication, economic resilience, intelligence cooperation and civil–military collaboration. This structure also allows for the study to go beyond the identification of hybrid threats and discuss viable methods that Pakistan can adopt to make its preparedness more robust to counter emerging multidimensional security threats (Naseeb, 2026).

Theoretical Relevance to the Study

This study is based on the three theories of stability – instability paradox, regional security complex theory, and national resilience framework to provide a comprehensive analytical base. The Stability–Instability Paradox is the rationale behind the escalation of strategic competition played within the realm of conventional warfare; RSCT is the understanding of how regional dynamics influence Pakistan's security environment; and the National Resilience Framework is the institutional and societal capacities to effectively resist hybrid threats. These viewpoints give a proper theoretical framework to examine new hybrid threats and formulate policy recommendations for enhancing Pakistan's national security (Ali, 2026).

4. Research Methodology

This study follows the qualitative research approach to analysis the changing character of hybrid warfare and its implications for national security of Pakistan. A qualitative approach is suitable as it is used to gain insight into complex strategic phenomena, to interpret the new security challenges, and to scrutinize policy reactions, and therefore not quantitative techniques are used. The research uses mainly descriptive and analytical approaches in explaining the multidimensionality of hybrid warfare and its effects on Pakistan's political, military, economic, cyber, informational and diplomatic security (Creswell, 2018).

The study focuses solely on secondary data derived from peer-reviewed journal articles, academic books, government policy documents, reports of international organizations, strategic studies institutes and official publications of

national strategic affairs and cyber security and hybrid warfare. Special attention has been given to the most recent scientific publications from the last ten years, to make sure that the considerations are oriented to the current state of the art in the field of hybrid warfare and new security issues (Snyder, 2019).

The descriptive-analytical and thematic content analysis methods were used in analyzing the data. The literature review was systematic and a thorough search was done to find out the common themes in the evolution of hybrid warfare, the new hybrid threats of today, Pakistan's national security challenges, and national resilience. Themes were then analysed according to analytical categories to explore the correlation between hybrid threats and the overall security scenario of Pakistan. This strategy allowed the study to integrate various different views from academics into a unified analysis (Braun & Clarke, 2021).

The theoretical approach to the findings is based on the Stability – Instability Paradox along with the theory of Regional Security Complex and the concept of National Resilience is used to assess Pakistan's ability to deal with multidimensional hybrid threats from a policy perspective. The incorporation of these approaches enables a comprehensive picture of the strategic drivers of hybrid warfare and the institutional responses needed to enhance national security, as outlined by Buzan & Wæver (2003).

The study has exhaustively covered all the emerging hybrid threats that have been facing Pakistan, but it has been qualitative only and has been relying on secondary sources. These findings are therefore reliant on the existing literature, and primary data collected by survey, interview and field observation is not included. However, the study benefits greatly from the use of recent academic literature and authoritative policy documents, as this helps to build the credibility of the research and also adds analytical depth to the study which will also serve as a good foundation for future empirical studies (Yin, 2018).

5. Emerging Hybrid Threats to Pakistan's National Security

In today's strategic scenario, Hybrid war is one of the most prominent non-conventional security

threats facing Pakistan. Hybrid warfare uses a combination of political, military, cyber, economic, informational, diplomatic and psychological tools, is coordinated and targets internal vulnerabilities with an aim of weakening the institutional capacity of a state, all of which are not traditionally used by the armed forces. The strategic importance of Pakistan coupled with the regional rivalries, changing geopolitical dynamics and national socio-political dynamics have all contributed to its vulnerability to multi-dimensional hybrid threats. The threats not only jeopardize national security but also affect public confidence, social cohesion, and economic stability and governance (Huşanu, 2026).

5.1 Information Warfare and Disinformation Campaigns

Information is a weapon in today's warfare. The growing use of digital media and social networking has created a new environment for the dissemination of misinformation, manipulation of opinion, and the heightening of political polarization in what has become a coordinated disinformation campaign. Over the years, Pakistan has seen a greater amount of information warfare aimed at eroding the trust of the people in the state institutions, sowing false notions, and exacerbating ethnic, religious, and political disharmony in the country. These campaigns aim to change the cognitive aspect of human behavior and they are one of the longest-running elements of hybrid warfare (Hatim, 2025).

5.2 Cyber Warfare and Critical Infrastructure Security

Cyber warfare is one of the fastest emerging aspects of hybrid warfare. Sectors traditionally considered critical infrastructure, financial institutions, communication networks, government databases and strategic organizations are now at risk of being targeted by cyberattacks aimed at disrupting and compromising essential services and sensitive information. With the continuous digital transformation of Pakistan, reliance on cyber infrastructure has grown significantly, creating more opportunities for vulnerabilities. Recent literature underscores the critical significance of cyber resilience as a new dimension of nation's security, as if the cyberattack is successful, the economic losses, institutional disruptions, and public uncertainty

can occur without the direct involvement of conventional military forces (Kausar 2026).

5.3 Proxy Warfare and Cross-Border Terrorism

The presence of proxy warfare in Pakistan's security environment has remained a significant aspect. Instead of direct military engagement, different parties tend to employ proxy groups, transnational terrorist groups and back channel assistance to achieve their strategic goals. These can lead to long-term instability through threats to internal security, interruptions in economic activity and a reallocating of national resources to counter-terrorism and internal security forces. Hybrid warfare often involves a blend of conventional war goals and unconventional tactics to undermine the security of the targeted country and its internal stability (Ali, 2025).

5.4 Economic Coercion and Strategic Competition

The economic instruments have gained a growing significance in the current concepts of hybrid warfare. To help shape political thinking and slow national development, various measures are used that include trade restrictions, financial pressure, investment uncertainty, sanctions, and attempts to undermine strategic infrastructure projects. Pakistan's country projects like the China-Pakistan Economic Corridor (CPEC) have both economic and strategic importance and could be seen as a potential target in the wider geopolitical competition. Economic security has thus been linked to national security, with the need for a resilient financial system, diversified economic relationships, and sustainable development policies to mitigate external threats (Lal, 2025).

5.5 Political Polarization and Societal Fragmentation

Exploiting domestic vulnerabilities is one of the hallmarks of hybrid warfare. Political uncertainty, institutional scepticism, ethnic and sectarian divisions, and social polarisation allow external actors to exacerbate internal tensions through information manipulation and influence operations. Hybrid actors do not seek to make new divisions but rather draw on existing fault lines in society to tear apart the nation and undermine public trust in democratic institutions. The developments demonstrate the interplay between

domestic political stability and national security in current strategic environment (Naseeb, 2026).

5.6 Diplomatic and Legal Warfare (Lawfare)

Diplomatic and legal tools are now being used by hybrid warfare to help to shape international opinion and influence decision making in regional and global organisations. Diplomatic campaigns, litigious action, international lobbying and narratives of strategy are all common tools used to question the legitimacy of state policies and to minimize diplomatic space and build political pressure without using force. Examples of these strategies illustrate how contemporary interstate competition is now being fought in legal and normative fields where information, international law, and global public opinion are all important strategic tools of influence (Radzi, 2026).

5.7 Interconnected Nature of Emerging Hybrid Threats

The analysis illustrates that hybrid threats are not stand-alone security issues. Information warfare enhances cyber warfare, political instability makes people more vulnerable to disinformation, economic coercion increases institutional pressures, and proxy violence makes vehicles for overall strategic aims. This interwoven nature makes hybrid warfare even harder to deter than conventional warfare, and requires other measures to be taken against it. Hence, Pakistan's national security needs an integrated and multi-dimensional approach which will simultaneously focus on military preparedness, governance, cyber security, economic resilience, institutional effectiveness and societal cohesion (Ahmed, 2024).

6. Building National Resilience: A Comprehensive Framework for Countering Hybrid Threats

Hybrid warfare is a multidimensional phenomenon, which shows that traditional military capabilities are not enough to safeguard national security. Modern hybrid threats simultaneously attack political institutions, economic systems, cyberspace, information environments, diplomatic relations and social cohesion. Thus, there is a need for an integrated national resilience strategy which would improve institutional capacity and the state's resilience capabilities to foresee, prepare, respond and

recuperate from multiple dimensions of threats faced by Pakistan. The concept of the national resilience should therefore not be only a defensive security concept, but should also be considered as a strategic national objective (Huşanu, 2026).

6.1 Strengthening Institutional Capacity and Good Governance

The first line of resistance against hybrid threats is the strong and effective institutions. Good management, effective public administration, transparency, accountability, rule of law, and efficient implementation of policies diminish possibilities for outside parties to take advantage of internal vulnerabilities. There should be an improvement in the institutional coordination of civilian agencies, intelligence services, law enforcement and the armed forces to ensure timely information sharing and coordination in the face of new hybrid challenges. The resilience of institutions in the end will build confidence in the public and add stability to the nation (Kausar, 2026).

6.2 Enhancing National Cyber Security

Cyber resilience is now an essential part of national security. Pakistan needs to further enhance its cyber security framework, by upgrading its digital infrastructure, investing in cyber defence technologies, enhancing its threat intelligence capabilities and building greater partnerships between the public sector, academia, and the private sector. Conducting regular evaluations of cyber risks, establishing response plans, and capacity-building initiatives will markedly enhance the country's capacity to prevent and counter more advanced cyberattacks on critical national infrastructure (Hatim, 2025).

6.3 Strategic Communication and Counter-Disinformation

Information warfare is now one of the most prevalent aspects of hybrid warfare. A coordinated strategic communication policy is needed in Pakistan to address misinformation, disinformation and hostile propaganda by providing timely, credible and evidence-informed public communication. Government bodies need to increase cooperation with responsible media bodies, online spaces, schools and civil society, to foster media literacy, fact-checking tools and awareness about manipulation of information. For

the cohesion of a nation and its democratic stability, it is critical to build social resilience against disinformation (Ali, 2026).

6.4 Economic Security and Critical Infrastructure Protection

Economic Resilience is one of the most important aspects of a nation's overall national security. Sustainable economic growth, diversified trade relations, energy security, financial stability, and securing strategic infrastructure decrease countries' vulnerability to external pressure and economic coercion. Special focus should be given to the integrated risk management and security planning of critical infrastructure such as energy production facilities, communication infrastructure, transportation infrastructure, financial infrastructure, and strategically important development initiatives (Lal, 2025).

6.5 Civil–Military Coordination and Whole-of-Nation Approach

Responses to hybrid warfare must go beyond traditional military institutions. National resilience relies on strong collaboration between civilian leadership, the military, intelligence services, the provincial government, academia, the private sector, the media and civil society. Whole-of-government, whole-of-nation (WG-WN) approach to information sharing and institutional coordination, crisis preparedness and national consensus during strategic uncertainty. This co-operation boosts Pakistan's capability in combating external aggression and internal hybrid threats (Naseeb, 2026).

6.6 Regional Diplomacy and International Cooperation

Pakistan needs to focus on the diplomacy and cooperation in the region, particularly with its partners in the international community in the areas of cyber security, counter-terrorism, intelligence sharing, financial regulation, and strategic communication to further enhance the response against hybrid threats. Close cooperation with regional groups and bilateral cooperation can support knowledge sharing, joint capacity development and joint responses to new challenges in the field of hybrid threats. Confidence-building measures are also a part of diplomatic engagement that helps ensure that there is no miscalculation on the part of the

countries in South Asia (Radzi, 2026).

6.7 A National Resilience Framework for Pakistan

Based on the preceding analysis, this study proposes an integrated national resilience framework consisting of seven mutually reinforcing pillars:

1. Effective governance and institutional resilience
2. Comprehensive cyber security and digital resilience
3. Strategic communication and information integrity
4. Economic security and critical infrastructure protection
5. Civil–military coordination and intelligence integration
6. Regional diplomacy and international cooperation
7. Societal cohesion, public awareness, and community resilience

The success of this approach relies on the ongoing political support, coordination among institutions, allocation of resources, and adaptation to the changing nature of hybrid warfare. However, Pakistan cannot solely depend on the traditional defence mechanism to safeguard its country's interests under all conditions, instead resilient institutions need to be established that can protect the country's interests in political, military, economic, cyber, informational and diplomatic arenas (Ahmed, 2024).

7. Policy Recommendations

Pakistan should develop an all-encompassing National Hybrid Warfare Strategy, which would cover both military and political, economic, cyber, informational and diplomatic dimensions and be part of a national security strategy. At the same time, the government needs to improve the national cyber security architecture by increasing investments in the development of advanced cyber security technologies, protection of digital infrastructure, the development of cyber defence intelligence and special training of human resources in the field of cyber security. It is advisable to strengthen the coordination of civilian agencies, intelligence agencies, law enforcement agencies and the armed forces in

order to optimize national preparedness in the face of multidimensional threats. Ensuring effective strategic communication mechanism to refute misinformation, disinformation and hostile propaganda and to strengthen credible public communication and media literacy in Pakistan should also be ensured. More focus needs to be placed on the protection of critical national infrastructure, economic resilience, increasing regional and international cooperation, and the need for a whole-of-government and whole-of-society approach to national security. Moreover, it is important that universities, think tanks and strategic research institutions are encouraged to conduct ongoing research on hybrid warfare for the purpose of evidence-based policy making. All these measures will have a significant impact on the national resilience and capacity of the country to proactively prepare for, endure, and react to the new hybrid threats.

8. Conclusion

The blending of conventional and non-conventional weapons and means in conflict across military, political, economic, cyber, informational and diplomatic fields has become one of the most prominent security issues in the twenty-first century – what is now called hybrid warfare. The hybrid threats differ from traditional wars in exploiting the vulnerabilities of a state and attacking it through coordinated and sometimes “deniable” actions, which are becoming more difficult to detect, deter and counter. The discussion in this study has shown that Pakistan's national security landscape is becoming more and more affected by multidimensional hybrid threats such as cyber threats, disinformation campaigns, proxy war, economic coercion, political polarization and diplomatic competition. These interrelated issues impact not only on the defence sector, but on governance, institutional effectiveness, economic stability and social cohesion.

The study also concludes that while such

traditional military means are crucial for national security, they are not adequate to combat the new type of hybrid warfare. Based on the Stability–Instability Paradox, Regional Security Complex Theory, and the National Resilience concept, this study shows that addressing hybrid threats needs an integrated response, both military and non-military, which includes good governance, cyber resilience, strategic communication, economic security, institutional coordination, and public trust. Improving these interrelated pillars will strengthen Pakistan's ability to predict the upcoming hybrid threats, resist them, adjust to them, and recover from them, thus protecting its sovereignty and long-term national security interests (Huşanu, 2026).

The study is an addition to the previous literature by assessing the concept of hybrid warfare from Pakistani national security's perspective and by introducing a multidimensional national resilience framework for Pakistan in light of strategic environment. This research takes a multi-faceted approach to the study of hybrid warfare, combining political, military, economic, cyber, informational, diplomatic and societal aspects in a single analytical framework, as opposed to studies that focus on a single dimension of security. The study's results, in this way, have theoretical significance and practical applicability particularly for those interested in understanding and addressing the changing nature of hybrid battle (Radzi, 2026).

However, the study has its limitations as it has been carried out using qualitative analysis and secondary data. Future studies could include empirical evidence in the form of interviews, surveys, and case studies of policymakers, security experts, military personnel, and cyber professionals. Comparative studies would also help to enhance scholarship on the hybrid threats faced by Pakistan and other countries in the world and help formulate better national responses in a complex global security context (Kausar, 2026).

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

- Ali, A. (2022). Challenges for the conventional deterrence of Pakistan in the post-2019 security situations: Options and choices. *Scandic Journal of Advanced Research and Reviews*. <https://doi.org/10.55966/sjarr.2022.3.3.0054>
- Aliyev, D. (2024). Hybrid warfare in the context of information confrontation. *Science. Culture. Society*. <https://doi.org/10.19181/nko.2024.30.4.1>
- Baig, M. A., & Ali, M. (2023). Hybrid warfare on Pakistan: Examining the determinants and impact. *Journal of Peace and Diplomacy*. <https://doi.org/10.59111/jpd.004.01.022>
- Bashir, H., Zarish, W., & Malik, R. (2024). The role of AI in hybrid warfare: A case study of Pakistan's cybersecurity landscape. *Global Strategic & Securities Studies Review*. [https://doi.org/10.31703/gsssr.2024\(IX-I\).08](https://doi.org/10.31703/gsssr.2024(IX-I).08)
- Çalışkan, M. (2019). Hybrid warfare through the lens of strategic theory. *Defense & Security Analysis*, 35. <https://doi.org/10.1080/14751798.2019.1565364>
- Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid war: High-tech, information and cyber conflicts. *Connections: The Quarterly Journal*, 16. <https://doi.org/10.11610/connections.16.2.01>
- Hatim, M., Irfan, A., Ranjha, E. U., Shah, H., & Ahmad, M. (2025). Hybrid conflict in the 21st century: Pakistan's security dilemmas and responses. *Social Science Review Archives*. <https://doi.org/10.70670/sra.v3i2.684>
- Huşanu, M. (2026). Aspects of hybrid warfare in the dynamics of its manifestation forms and action mechanisms. *Bulletin of "Carol I" National Defence University*. <https://doi.org/10.53477/2284-9378-26-12>
- Hussain, M., & Naqvi, S. I. A. (2024). Indo-Pakistan rivalry and integrated ring balancing: Prospects and challenges to regional stability in South Asia. *Asian Journal of Political Science*, 33. <https://doi.org/10.1080/02185377.2024.2386663>
- Jalil, H., & Ehsan, M. (2023). Hybrid warfare: Emerging challenges for Pakistan. *Journal of Contemporary Studies*. <https://doi.org/10.54690/jcs.v11i2.234>
- Kausar, A., & Iqbal, M. (2026). Hybrid warfare, state responsibility, and interstate conflict in South Asia: Evidence from India-Pakistan relations. *Inverge Journal of Social Sciences*. <https://doi.org/10.63544/ijss.v5i2.268>
- Lal, M. S. (2025). The Iran-Saudi cyber and hybrid warfare: Analyzing the strategic implications for Pakistan. *Journal of Political Stability Archive*. <https://doi.org/10.63468/jpsa.3.1.04>
- Mali, P. (2025). India's cyber warfare options against Pakistan: A strategic analysis. *International Journal for Multidisciplinary Research*. <https://doi.org/10.36948/IJFMR.2025.V07I02.43343>
- Naseeb, J., & Kazmi, S. S. (2026). Cyber warfare and strategic stability in South Asia: A securitization analysis of India-Pakistan cyber incidents (2016–2025). *Journal of Political Stability Archive*. <https://doi.org/10.63468/jpsa.4.1.44>
- Radzi, S. A. M., & Jaafar, F. (2026). The Iron Cage: Security dilemma dynamic driving the India-Pakistan conflict. *Malaysian Journal of History, Politics and Strategic Studies*. <https://doi.org/10.17576/jebat.2026.5301.07>