Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Hybrid Warfare and China-Pakistan Economic Corridor (CPEC): How China Helps Pakistan Manage Information Threats

Naqib Ullah Khan
PhD, Political Science Scholar, Qurtuba University, Peshawar, KPK

Muhammad Sohail Khan
PhD, Political Science Scholar, Qurtuba University, Peshawar, KPK

Waqas Jan Durrani (Correspondence Author)
PhD, Political Science Scholar, Qurtuba University, Peshawar, KPK
Email: waqas.durrani@bkuc.edu.pk

Mian Muhammad Khan
Department of Management Sciences and Commerce, Bacha Khan University Charsadda KPK

ABSTRACT

China-Pakistan Economic Corridor (CPEC) has become one of the core elements of the regional connectivity and the long-term economic policy of Pakistan. But it has also been placed in the target of hybrid warfare by combining information operations, disinformation campaigns, and cyber-enabled propaganda, because of its strategic value as well. Such threats are supposed to erode public confidence in the CPEC, make relations between China and Pakistan hostile, as well as disrupt the security environment in Pakistan. In turn, China has been more involved in assisting Pakistan by undertaking sophisticated cyber partnerships, information protection education, online infrastructure defense, and collaborative anti-disinformation systems. In this paper, the authors explore the idea of hybrid warfare against CPEC, the character of information threat, and the changing China-Pakistan partnership in order to overcome such adversity. It holds that Chinese support not only makes Pakistan more resilient in terms of cyber-attacks, but it is also empowering its strategic communication and narrative control in response to advanced information warfare campaigns. The results show that to combat hybrid threats, a comprehensive strategy is needed, including technological cooperation, the capacity of institutions, and active digital diplomacy to protect CPEC against the future actions of destabilizing information.

Keywords: CPEC, Hybrid Warfare, Narrative Management, Crisis Management, China-Pakistan Relations, Information Warfare, Disinformation, Strategic Communication, Digital Security, Connectivity Initiatives.

Introduction

One of the most strategically significant aspects of the Belt and Road Initiative (BRI) is China-Pakistan Economic Corridor (CPEC) where China and Pakistan link their

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Gwadar Port and Xinjiang province respectively. CPEC is a groundbreaking economic opportunity in Pakistan being a multibillion dollars connectivity and infrastructure initiative. However, its tactical importance has also predisposed it to hybrid warfare in situations when the sides employ non-kinetic weapons such as disinformation, cyber-attacks and control of stories to destabilize Pakistan and the relations between China and Pakistan (Clarke, M., et al., 2017).

The geopolitical tussle in the South Asian region, especially between Pakistan and India, has increased the fighting of the hybrid war against CPEC. The scholars claim that the active application of disinformation campaigns, influencing the discourse, and promoting digital propaganda have served to discredit CPEC and instill mistrust on the level of the population and discredit the institutions of the state. Such information activities should serve to sow doubt about the destiny of the Pakistani economy, incite the regional indignation, and discourage the foreign investment by making CPEC appear greedy or unsustainable.

Pakistan is very vulnerable to this information environment. Research shows that anti-CPEC propaganda often overlaps with the internal fault lines in Pakistan including ethnic conflicts in Baluchistan, the governance problem, and political polarization. This internal instability and external information interplay predisposes Pakistan to hybrid threats in a very particular way. Social media distribution of coordinated disinformation that is usually enhanced by adversarial actors in the region has complicated the security situation in Pakistan further (Afzaal, M., 2020).

Upon understanding these problems, China has become more cooperative with Pakistan in cyber defense, digital infrastructure protection, media coordination, and counter-disinformation measures. Analysts point out that the experience that China has had in dealing with information security and cyber threats offers Pakistan with technical capacity, training, and political assistance to better deal with information warfare. This collaboration is representative of the greater strategic goal of China protecting BRI projects against hybrid threats and providing the long-term sustainability of CPEC (Rolland, N., 2017).

On the whole, hybrid warfare against CPEC accentuates the transformation of warfare in the 21st century. Rather than military face-off, the opponents of military conflict use manipulation of information to undermine strategic alliances and unstable states. With Pakistan still trying to navigate through this unfriendly information space, the role of China in harnessing the hybrid threats has taken on the contemporary importance of maintaining the CPEC momentum and strengthening the region with its stability. These dynamics are important in assessing the capability of Pakistan and China to protect their mutual economic and strategic interests together.

Literature Review

Hybrid warfare has been conceptualized by scholars as a fusion of conventional, irregular and cyber/information operations which aim to accomplish strategic goals at a level below the level of open war. The term was popularized by Frank G. Hoffman, who emphasized the potential of hybrid threats to combine military and non-military capabilities (economic pressure, insurgency, information operations) to form complex security environments that cannot be effectively dealt with using conventional defence measures. More contemporary therapies are based on the primacy of

Online ISSN 3007-3197
Print ISSN 3007-3189

information and influence processes in hybrid strategies, which holds that narrative control and reputational loss can be as telling as kinetic action. (Rid, T., 2020).

The information disorder and disinformation literature offers a viable model of the manner in which hybrid campaigns affect the opinion of the people and social cohesion. According to a widely referenced interdisciplinary review, Wardle and Derakhshan distinguish between disinformation, misinformation, and malinformation and visualizes the actors, motives, and mechanics of information dissemination that form the basis of contemporary information actions. This literature is indispensable when investigating how anti-project messages can be reinforced in online platforms, bots, and coordinated networks, and thus discredit popular support of projects such as CPEC (Wardle, C., & Derakhshan, H., 2017).

The Belt and Road Initiative (BRI) and the China Pakistan Economic Corridor (CPEC) are analyzed as these projects are placed in the context of great-power politics and development in the region. As Andrew Small and others demonstrate, CPEC is both an economic development initiative and a geopolitical tool at once, thus, becoming a strategic object of attack to any actors who want to disrupt China-Pakistan cooperation. Greater attention to CPEC, however, is based on the belief that political dissatisfaction, localized insurgent actions (especially in Balochistan), and governance failures provide the fertile ground of narrative attacks and hybrid actions that undermine the popularity of the corridor (Zingel, W. P., 2020).

Cyber operation and norm studies contribute to a legal and technical context to the analysis of hybrid-threats. The Tallinn Manual 2.0 is a seminal, practitioner-focused examination of the application of international law in situations of cyber operations and guidance on how states should respond, who should be attributed and what should be countermeasured; this is directly relevant when states or proxies launch cyber-attacks on infrastructure or information systems related to CPEC. There is growing agreement among scholars and policy analysts that securing large transnational projects needs hardening of industrial control systems but also tough information ecosystems and legal frameworks to discourage and react to hostile influence operations enabled by cyber-technology (Schmitt, M. N., 2017).

A number of policy-based studies consider how China goes about protection of BRI projects and how it reflects in cooperation with host states. Think tanks and scholars report and analyze that the Chinese mechanism of securing foreign projects comprises technical assistance (cyber-security, surveillance and data protection), institutional cooperation (security dialogues, training), and information management, which can be used by Pakistan as a measure to counter hybrid campaigns against CPEC. Nonetheless, literature also raises the issue of governance, sovereignty and rights-related concerns when the foreign actors influence the way the domestic countries respond to information and cyber policies (Farwa, U., 2018).

Lastly, the regional analysis specializing in Pakistan specifically indicates structural weaknesses in the form of political polarization, lack of governance in certain provinces, and lack of media literacy, which are exploited by the hybrid actors. Empirical evidence indicates that disinformation stories regarding international projects are more easily accepted in environments where there exist local resentments and anxieties over the economy. According to that literature, a hybrid response, which includes technical cyber-security solutions, media literacy initiatives, and local

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

development inclusion to decrease vulnerability to hybrid influence, is recommended (Afzaal, M., 2020).

Research Objectives

The main aim of the present research is to discuss the use of hybrid warfare tactics such as disinformation campaigns, cyber manipulation as well as narrative distortion to weaken the China-Pakistan Economic Corridor (CPEC) and influence the information space of Pakistan. The study will also endeavor to determine how the co-operation of China can be used to increase capacity of Pakistan to stem such information-based threats by building a robust cyber-security system, electronic governance systems and strategic communication systems. Also, the paper will evaluate the performance of bilateral China-Pakistan programs to counter the hybrid threats and preserve the strategic and economic sustainability of CPEC. The other important aim is to establish the institutional, political and technological issues that Pakistan is encountering when it comes to complete utilization of Chinese aid in the management of information warfare. Finally, the study will suggest evidence-based policy changes to make Pakistan resistant to hybrid information threats and help to secure and provide long-term stability in CPEC.

Research Questions

What is the nature of the attack on CPEC by hybrid warfare tactics (disinformation, cyber manipulation, and narrative framing) and how it affects the environment of information within the domestic context of Pakistan?

How does China help Pakistan counter the information threats by offering cyber-security cooperation, digital governance resources, and strategic communications assistance?

To what extent are the joint China-Pakistan mechanisms effective in reducing hybrid information threats, and what are the limitations to full benefit of this cooperation by Pakistan?

Research Methodology

The paper will utilize a qualitative research approach to examine the nature of hybrid warfare against CPEC and evaluate the role that China plays in helping Pakistan to counter the threat of information. There is a descriptive and analytical research design to investigate the ways in which disinformation, cyber influence campaigns and strategic narratives influence the security environment in Pakistan. The study is based mostly on the sources of secondary data, i.e., peer-reviewed journal articles, policy papers, think-tank reports, official government documents, and the publications by the National Bureau of Asian Research (NBR) and the Carnegie Endowment of International Peace and the Pakistan Institute of Peace Studies (PIPS). The systematic content analysis is chosen as the way to collect the data and identify the themes, patterns, and strategies related to hybrid warfare and counter-information measures. The methodology also incorporates documentary analysis to assess China-Pakistan cooperative delivery systems in the area of cyber-security, digital infrastructure guard, and planning communications. This research takes an interpretivist strategy, which gives an opportunity to learn more about the political, strategic, and technological

Online ISSN 3007-3197
Print ISSN 3007-3189

environment that informs hybrid threats and responses. This methodology will provide a holistic and evidence-based evaluation of the role of China in helping Pakistan to deal with information threats in connection with CPEC.

Research Gap

Despite the available written sources on China-Pakistan economic collaboration and China-Pakistan Economic Corridor (CPEC) security, the issue of hybrid warfare and information threats against this strategic initiative is not under scrutiny. The role of disinformation and cyber operations, as well as influence campaigns are understudied when it comes to CPEC, although most studies focus on conventional security issues, terrorism, and geopolitical rivalry. Moreover, although the assistance provided by China to Pakistan in the form of infrastructural and financial aid is well-reported, the literature on analyzing the strategic aid offered by China in dealing with information threats and hybrid wars is limited. Literature does not incorporate much interdisciplinary approaches that merge cyber-security, strategic communication and political analysis to assess how Pakistan manages to curb these threats in collaboration with the Chinese. Thus, the research paper fills a critical gap by considering the interaction of hybrid threats, information security, and the role of the Chinese in helping Pakistan, which gives both empirical and strategic policy ideas.

The Concept of Hybrid Warfare

A multidimensional concept of warfare that integrates standard military operations along with irregular ones, cyber-attacks, disinformation campaigns, economic pressure, and political subversion, hybrid warfare is a complicated phenomenon. As opposed to a traditional warfare, the hybrid strategies are structured to take advantage of the vulnerabilities of the states during peacetime as well as during conflict situations and leave the traditional defense mechanisms to react ineffectively. The hybrid warfare in the South Asian context is usually aimed at disrupting the governance systems, as well as the information and perception systems of the masses and disrupting critical infrastructure to destabilize the government systems and shape its strategic decisions. Distance in the breadth of operation, i.e., military, economic, political, and informational potential, contributes to the fact that hybrid threats are especially relevant to Pakistan, given its strategic activity such as the China-Pakistan Economic Corridor (CPEC) (Kofman, M., & Rojansky, M., 2015).

One of the most essential parts of the hybrid warfare is information operations which involve propaganda, disinformation, cyber-attacks and manipulation of the media. These activities are designed to influence the narratives, crowd thinking, and erosion of confidence in institutions without direct conflict. In the case of Pakistan, which is also active in high profile initiatives within the framework of CPEC, information threat can be used against both domestic and foreign audiences, influencing investor trust, publicity, and stability in the region. The use of technological tools, social media and transnational networks to spread misguided information and cause confusion makes information management an essential part of national security strategy, hence the use of hybrid adversaries (Hoffman, F. G., 2014).

The non-state actors, including extremist groups, organized crime networks, and proxy actors, are also involved in hybrid warfare and cooperate or support the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

strategies supported by the state to increase instability. These actors are able to attack in specific places, engage in cyber-attacks, or organized propaganda that support an overall strategic effort. This implies that Pakistan will need to find mechanisms of detecting, defusing, and canceling such activities that sometimes lie between the war and the peacetime system of governance that also requires adaptive security strategies (Richelson, J. T., 2018).

Hybrid warfare is relevant when it comes to the study of the role that China played in the support of Pakistan in this field. The Chinese experience as far as the issue of information security, cyber governance and strategic communication are concerned can be used as a model, which Pakistan can apply in order to be resilient to hybrid threats, particularly in the CPEC routes. Pakistan can deal with weaknesses and provide the safeguarding of economic and strategic interests against intruders within and beyond the state that engage in hybrid operations through the integration of technology solutions, intelligence and strategic planning.

CPEC as a Target of Hybrid War

The China-Pakistan Economic Corridor (CPEC) is one of the flagship projects of the Belt and Road Initiative (BRI) of China and has become a strategic and economic resource when it comes to both China and Pakistan. Nevertheless, being a major target, it is also a prime target of hybrid warfare activities, such as cyber-attacks, disinformation campaigns, sabotage, and insurgent activities. The objective of hybrid actors is to destabilize, compromise the security, and prosperity of CPEC projects by taking advantage of political, social, and ethnic conflicts in the corridor to stall or derail the growth of infrastructure. Besides posing a risk to economic investments, such attacks have the potential to significantly undermine the trust of the citizens in the government to secure national projects, as a result disrupting regional governance (Small, A., 2014).

CPEC is also heavily worried about cyber-security vulnerabilities since critical infrastructure e.g. energy pipelines, transport networks, communication systems are prone to hacking, malware attacks, and digital espionage. These systems may be modified or interfered with by the hybrid adversaries, preconditioning operational delays and financial losses, and using digital platforms to spread false information on CPEC social and environmental effects. These kinds of campaigns may impact local communities, investors and international onlookers in a manner that may influence perceptions over continuity of projects and regional partnerships (Surahio, M. K., et al. 2022).

Other than cyber threats, CPEC is also prone to physical sabotage and insurgency, especially where there has been a history of unrest or political instability in the region. Hybrid warfare techniques usually use proxy targets or radicals to strike constructions sites, transportation convoys or security posts to indicate to the local and foreign publics that the corridor is not secure. Such tactics are aimed at establishing some uncertainty and fear which affects not only the logistics of operations but also the diplomatic relations with China. In the case of Pakistan, it is necessary to have sufficient security systems on the CPEC track to ensure that these hybrid threats do not evolve into full-fledged crises (Kuszewska, A., & Nitza-Makowska, A., 2021).

The threats of CPEC in a hybrid form are not restricted to either physical or cyber-

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

realms only but spread to economic and informational warfare where the opponents may seek to manipulate international funding bodies, media outlets, and local stakeholders into doubting the legitimacy or advantages of the corridor. These complex issues can only be dealt with as a coordinated effort of intelligence, diplomatic interventions, and technological interventions and in most cases through Chinese alleviates acting as advisors regarding mitigation of risks and strategic communication. The successful management of the hybrid threats will guarantee that CPEC remains a catalyst of the economical development and regional connectivity and enhances the connection between Pakistan and China at the strategic level (Small, A., 2014).

CPEC Information Warfare and Disinformation.

China-Pakistan Economic Corridor (CPEC) has come to become a subject of the information warfare, with the participants engaging digital platforms, social networks, and traditional mass media to alter the opinion of citizens, create political pressure, and weaken the legitimacy of the initiative. Disinformation campaigns usually overstate the risks, emphasize the purported environmental negative impacts, or suggest that the corridor is skewed toward foreign interests to the disadvantage of the local communities. These kinds of narratives are being strategically used to undermine trust of people, destabilize political support, and cause tension between Pakistan and China. The ubiquitous character of these campaigns strengthens local frustrations that hybrid enemies can capitalize on to develop tensions in the society (Kalpokas, I., 2017).

One of the main fields of battle of the CPEC-related disinformation is social media, in which fake news, photoshopped photos, and misinformation can reach millions of people in a few hours. The information asymmetry and low digital literacy rates allow hybrid actors to manipulate the perception of security, economic gains, and the effectiveness of government and, therefore, both domestic opinion and an international stakeholder. Not only does this warfare affect the socio-political climate of the corridor, the investor inclination is also influenced as a result of which it may affect foreign direct investment, and the economic feasibility of CPEC projects overall (Maqsood, A., 2025).

In addition, well timed campaigns seek to instill the doubts regarding the institutional ability of Pakistan in safeguarding the corridor against threats within and outside the nation. Cyber intrusion is usually accompanied by disinformation and propaganda, as well as selective coverage to create an impression of unstable conditions, overstating violence, project delays, or corruption. This poses a multidimensional challenge to the Pakistani authorities, where the security of physical infrastructure is not limited to merely securing physical infrastructure, but also proactively control the narratives to defeat disinformation. In order to curb these threats, Pakistan in conjunction with China has been investing more and more in strategic communication, digital monitoring and public awareness. Active communication with the local population, timely reporting on the development of the project, and timely counter-messaging are essential in dispelling disinformation and ensuring trust in CPEC projects. Information warfare is now viewed as a key factor to physical security to ensure the continuity of the corridor and the security of the strategic partnership between China and Pakistan (Saud, A., & Kazim, N., 2022).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

China's Role in Supporting Pakistan's Information Security

China has turned out to be a strategic partner in strengthening the Pakistan information security, especially on how to protect the China-Pakistan Economic Corridor (CPEC) against the hybrid and cyber threats. China offers technical support, practices, and policies to Pakistani organizations to identify, avert, and manage disinformation and cyber-attacks against critical infrastructure through its comprehensive cyber-security and digital governance experience. This collaboration is part of a wider strategic alignment where both the countries are aware of the fact that information dangers have the potential to disrupt economic as well as geopolitical stability should they be unchecked (Anwar, U., & Atif, M., 2025.

Among the most important ones is the transfer of cyber-security technologies and monitoring systems enabling Pakistan to monitor online stories, detects disinformation campaign, and takes immediate action against misinformation against CPEC projects. Chinese specialists also attend capacity building trainings of Pakistani government bureaucracies that train on digital intelligence, threats analysis and secure communications. This kind of cooperation will not only empower Pakistan and strengthen its defenses but also will build trust between the two countries and strengthen the strategic alliance between them (Khan, S. U., et al., 2025).

China has not only been an advocate in technical aspects but also in policies that govern information. As a leader in its national experience of how to handle digital propaganda and how to deal with hybrid threats, China can help Pakistan to build extensive systems of digital security, communicational, and crisis management. It assists Pakistani authorities to actively disrupt disinformation activities, organize inter-agency operations, and keep the people in CPEC initiatives loyal. Also, collaborative studies, training of seminars, and simulation training constitute an essential aspect of China-Pakistan partnership in information security. Such activities are to predict emerging threats, architect early-warning systems, and strengthen against the advanced hybrid operations. China can enhance the capacity of Pakistan to protect its strategic economic initiatives and the region wide security conditions by combining technology, policy, as well as capacity-building (Ahmed, S., 2024).

Technological and Cyber Collaboration Between China and Pakistan

China and Pakistan have intensified their collaboration in the technological and cyber field especially in terms of safeguarding the China-Pakistan Economic Corridor (CPEC) and vital national infrastructures against hybrid threats. The collaboration includes the creation of sophisticated cyber-security systems, digital monitoring tools, and safe communication systems that will allow Pakistan to identify and act upon cyber-attacks and information manipulation campaigns successfully. By utilizing the experience of China in cyber defense and the advanced technologies, Pakistan enhances its resiliency against the threats of cyber interruptions that may disrupt both the economic projects and the national security. One of the main points of this cooperation is the creation of cyber surveillance posts and online control centres together. They are sites that provide real time research on cyber threats, coordination of the government in departments and instantaneous reaction to online attacks on strategic projects. China also provides hardware solutions and software platforms and training programs to Pakistani cyber-security specialists, which enhance their

Online ISSN 3007-3197
Print ISSN 3007-3189

professional skills and readiness to operate. This partnership emphasizes the fact that cyber-security is not a technical challenge at best but a strategic requirement to continue with the regional drive of CPEC initiative (Ullah, F., 2024).

In addition to the technical infrastructure, China and Pakistan are taking part in the research and development activities on AI, data analytics, and secure network technologies. Collaborative projects will help determine the vulnerabilities of the digital systems, simulate possible situations of the cyber-attacks, and create effective countermeasures. This collaboration makes sure that Pakistan is dynamic enough to keep up with new threats at the same time as promoting the development of technology in the field of cyber-security inside the country. There is the collaboration through policy and strategic direction, in which China will support Pakistan in developing cyber-security laws, threat response policies and strategies to employ cyber diplomacy internationally. Such combinatory policy, technology, and human resource development helps to make Pakistan more resilient to cyber threats, and at the same time, it enhances the bilateral strategic alliance and creates a stable cyber situation in the region. (Zhao, X., 025).

Impact of Hybrid Warfare on Pakistan's National Security

The hybrid warfare has now emerged as a major menace to the national security of Pakistan as the style of fighting is a combination of both conventional and unconventional methods such as cyber-attack, manipulation of information, and disrupting economies. All these multi-dimensional threats sabotage state institutions, political instability, and put Pakistan at a disadvantage when it comes to control over strategic projects, including China-Pakistan Economic Corridor (CPEC). The hybrid operations tend to take advantage of the social media, propaganda networks, and misinformation campaigns, which increase internal divisions, and perpetuate extremism, placing Pakistan at the risk of both domestic and foreign security threats. It is in the cyber aspect of the hybrid warfare that is of major concern to Pakistan where cyber-attacks on critical infrastructure, financial organizations/ institutions, and government digital networks can have spillover effects on national security. Such attacks are also secretive and tricky to trace and through them the enemies can cause tactical misunderstanding but not come out and fight. It follows that Pakistan has the twin task of securing its technological resources and refuting the strategic discourses of its antagonistic forces and needs a delicate combination of technical, intelligence, and policy answers (Ali, F., et al., 2025).

Pakistan has also been hit by hybrid warfare because the infrastructural works in the country, the energy supply lines, and the trade routes are targeted to cause financial instability. To illustrate, the illusionary propaganda against CPEC is capable of undermining investor trust and breaking international collaboration. Such a complex threat landscape pushes Pakistan to incorporate cyber security, communications, and intelligence coordination in its national As it is capable of minimizing the risks and easing the sustainability of the development projects. The impact of the hybrid war can also be transferred to the dynamics of the security in the region, as any attack on Pakistan can also have an extended impact on the stability in South and Central Asia. The fact that hybrid threats are connected to geopolitical competition highlights the need to make Pakistan more resilient at the national and international level and have

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

established a better relationship with China in particular so that the strategic interests of the country are not threatened and the region remains stable (Clary, C., et al., 2021).

China-Pakistan Joint Counter-Hybrid Strategies

The strategic relationship between China and Pakistan has been enhanced to respond to hybrid threats particularly those that threaten to impact the critical infrastructure such as the China-Pakistan Economic Corridor (CPEC). Multi-dimensional nature of hybrid warfare that entails cyber-attacks, information manipulation and economic repression, the two nations have focused their efforts towards setting up mutual intelligence sharing, cyber defense and strategic communications. Not only do these concerted zones reinforce the Pakistani government against the asymmetric threats, but they also offer sustainability and safety of major projects in both the economy and development. Cooperation in technologies and cyber-security is one of the key elements of the China-Pakistan counter-hybrid policy that implies the installation of advanced surveillance systems, network security measures, and online intelligence services. Combining the abilities of China to defend against cyber-attacks and the local intelligence capacities of Pakistan, the collaboration between the two countries forms an effective defense against disinformation campaigns, ransomware, and other cyber-attacks. This partnership does not only reduce the security risks in the short term, but also builds long term institutional capacity to respond to the emerging hybrid threats in Pakistan (Wolf, S. O., 2019).

The alliance also focuses on the importance of strategic communication and narrative management, as a measure to prevent misinformation and disinformation spread about Pakistan and CPEC. The two countries also organize the work of public diplomacy and media surveillance and social media intelligence activities to counter the destabilizing activity of the aggressive forces intending to affect the situation in the region. China and Pakistan may decrease the negative effects of hybrid operations by being proactive to manage the narratives and public perception to ensure the security of the society and safeguard the economic stability of the region. Counter-hybrid measures are also joint to capacity-building efforts and alignment of the policies so that the two countries can react to the hybrid threats in a variety of areas. This involves collaborative trainings, cyber-security conferences, and coordination through regional forums to enhance multilateral cooperation to fight asymmetric challenges. The long-term China-Pakistan partnership is an example of how strategic partnerships can contribute to the national security, safeguard initiatives of development, and promote regional stability in the face of hybrid warfare (Hussain, M., & Ahmed, S., 2021).

Challenges in Combating Hybrid Threats

Pakistan is challenged by a number of strategic and operational issues in countering the hybrid threats especially those against CPEC and other critical facilities. The complexity of hybrid warfare (consisting of cyber-attacks, disinformation, economic sabotage, and proxy warfare) makes it hard to react to it through conventional security and intelligence systems. There is a lack of technical capacity, inter-agency coordination, and the changing threat vectors which further add vulnerability to the

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

situation in Pakistan and require ongoing adaptation and investment in counter-hybrid mechanisms (Yamin, T., 2019).

One of the problems is infrastructure and capacity of cyber-security. Although Pakistan has been cooperating with China, the nation still has inadequate domestic cyber defense that is shared between federal and provincial organizations. The high rate of technological change in cyber threats and lack of expertise in the human resources would leave loopholes that could be exploited by the adversaries. Furthermore, the spread of online platforms and social media has simplified the process of organized disinformation attacks by hostile actors against the people and investor trust in such projects as CPEC (Aslam, H. A., 2025).

These intelligence constraints and information asymmetry also contribute to a weak capacity of Pakistan to counteract hybrid threats. Hybrid operations are created to be uncertain on purpose, and often those committing them do not identify themselves or use proxy groups. This complicates attribution and postpones measures of response in a timely manner. Military, intelligence, and civilian agencies need to coordinate effectively, which is essential but can be hampered by bureaucracy and inefficiency, absence of real-time sharing of intelligence, and political considerations. Pakistan is not the least, and it is confronted with the problems of geopolitical nature of the region, which complicates its counter-hybrid approaches. The presence of various state and non-state actors in the hybrid operation coupled with external demands by rival powers in the region makes the security environment a complex environment. It takes fine-tuning of policy and long-term sight to put domestic security concerns on the frontburner and at the same time, ensure that diplomatic and economic ties especially with China continue to be strong. These predicaments present the need to continue investing in capacity-building, strategic partnership, and policy development to protect national security in Pakistan against hybrid threats (Yamin, T., 2019).

Opportunities for Strengthening Cyber and Information Defense

Pakistan has a number of strategic tools to develop its cyber and information defense systems, especially by working with China as part of CPEC. The continued China-Pakistan collaboration provides an opportunity to access modern technologies of cyber-security, training opportunities and best practices that could assist Pakistan in developing a resilient digital infrastructure. Incorporate Chinese competencies in the cyber intelligence, artificial intelligence, and surveillance systems, Pakistan will be able to detect, prevent, and respond to complex hybrid threats against critical assets of the nation. One of the opportunities is in the area of capacity building and human resource development. The technical and analytical capabilities of Pakistani professionals can be enhanced with the help of investment in specialized training of cyber-security specialists, joint research projects and academic exchanges with Chinese organizations. This does not only enhance the ability to manage cyber events, but also enhances the strategic freedom of the nation in terms of formulating proper counter-hybrid strategies (Khan, K., et al., 2024).

Policy and regulatory frameworks are also another opportunity. The vulnerable situations can be eliminated by developing better laws on cybercrime, data protection, and information security and adhering to the international standards, and the coherent response towards the information warfare can be ensured. The previous experience

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

China had when organizing massive cyber activity and establishing effective information control systems can also be of great value to Pakistan to adhere to in its socio-political environment. Pakistan will be able to strengthen collaboration between the citizens and their private sector to achieve critical infrastructure. By working with technology companies, telecommunication companies and research organizations, a more coordinated and active defense environment will emerge. Government regulation and the involvement of the private sector in the industry can enhance the sharing of threat intelligence, create quick response, and create a cultural ethic of cyber-security awareness among the people of Pakistan. When planned, these opportunities have the potential to make the cyber and information defensive stance of Pakistan a major foundation of national security (Zhao, X., 2025).

Conclusion

The studies of the idea of hybrid warfare and CPEC draw our attention to the fact that the modern challenges in Pakistan were more sophisticated. Such combination of cyber-attack, disinformation and economic sabotage have also been directed at critical infrastructure and economic projects like CPEC in Pakistan. The said threats not only disrupt the economic stability but also may disrupt the national security and the relationship in the region.

One of the strategic assets became the contribution made by China to the information and cyber security in Pakistan. Pakistan has been able to improve its security system against high-tech hybrid threats through technological cooperation, exchange of information and capacity building programs. The alliance has also assisted Pakistan to implement high standard cyber constructs, policy, and model of best practices of both public and private cooperation that are required to safeguard the valuable national infrastructure.

There are still high chances of achieving cyber resilience. By investing in human resource development, regulatory improvement as well as strategic technological partnership with China, Pakistan will have the capability to establish a multi-layered as well as multi-tiered defense system that will be mobilized to respond to the emerging and current multi-dimensional threats. These efforts also result in the national security including stability and sustainability of the China-Pakistan Economic Corridor that is essential to the economic growth of Pakistan and the regional impact of the country.

In conclusion, the relationship between China and Pakistan is a rational and futuristic plan to a hybrid war on information and cyber threats management. Such common knowledge and resources can be utilized by Pakistan to make it less vulnerable and more strategic deterrence and attain the national and regional security objectives in a more competitive geopolitical environment.

Findings

CPEC as a Strategic Objective: China-Pakistan Economic Corridor has been identified as the most appropriate object of hybrid warfare due to its economic and geopolitical significant value. It is sabotaged by regular disinformation campaigns, cyber-attacks and propagandas.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 12 (2025)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Emerging of Information and Cyber Attacks: Cyber-attacks, social media manipulation, and misinformation are gradually becoming part of the hybrid attacks on Pakistan with the aim of manipulating the opinion of population and creating instability in the political field.

As a result of the Chinese aid during the war on terrorism, the Chinese have been providing important assistance to Pakistan to combat the hybrid threats through their support in form of technological equipment, intelligence sharing and capacity building programs to boost the cyber defense infrastructure in Pakistan.

Technological Cooperation Multilateral cooperation between China and Pakistan, including cyber war drills, secure communication systems and AI-driven threat detection have been found to be rather helpful to increase the ability of Pakistan to detect and suppress hybrid attacks.

Strengthening Policy and Regulatory: National strategies and policies have been formulated through the concerted efforts to defend critical information infrastructure against hybrid attacks.

Construction of Training programs and technical workshops with the help of Chinese have improved the human capital of Pakistan in the sphere of cyber defense, information security and the hybrid threat management.

Challenges Remain Significant: Pakistan is not free of challenges as it still has to resolve several challenges following the increased threat of hybrid threats, the lack of technological autonomy, and the high demand of better coordination between the governmental and non-governmental spheres.

Strategic Implications of national security: A sound mechanism to handle the hybrid threat with China assistance has helped Pakistan to boost its national security safeguarding its economic interests as well as its strategic position in the region.

Opportunities of Future Cooperation: The results indicate that the further enhancement of technological cooperation, intelligence sharing and policy alignment with China can contribute to an improvement of the resilience of Pakistan to hybrid warfare.

Hybrid Threats Affect the Opinion of the People: It is also shown that the campaigns of information warfare have a direct effect on the public opinion, and a set of strategic communication and counter-propaganda efforts is needed.

Recommendations

Build Capacity to Cyber and Information Security: To protect CPEC and other important projects against hybrid threats, Pakistan should invest in state-of-the-art cyber defense systems, secure communication channels, and AI-based threat-detecting systems.

Strengthen China-Pakistan Cooperation: The collaboration between China and Pakistan should be strengthened by increasing joint initiatives such as intelligence sharing, cyber-security drills, and technological innovation, among others, so that Pakistan is proactive in responding to new hybrid threats.

Create Comprehensive Counter-Disinformation Plans: The government must adopt national level plans to combat misinformation and propaganda such as media literacy, social media awareness as well as social media monitoring.

Online ISSN 3007-3197
Print ISSN 3007-3189

Capacity Building and Training: There must be constant training of the cyber-security professionals, government officials, and law enforcement professionals on cyber-security to enhance human capital in detecting, analyzing, and mitigating hybrid threats.

Strengthening of policy and regulations: Pakistan is advised to develop and revise laws and regulations to regulate cyber operations, critical infrastructure protection and transnational information threats to establish a legal structure that promotes the national security.

Public-Private Sector Coordination: It is recommended to promote cooperation between the public institutions and the entities based in the private sector engaged in the CPEC projects in order to have a coordinated response to the cyber-attacks, information campaigns, and other hybrid threats.

Early Warning and Rapid Response Mechanisms: An early-warning and rapid response mechanism through the development of specialized centers to analyze threats, respond quickly, and effectively address hybrid warfare strategies will assist Pakistan to anticipate, detect, and respond effectively to hybrid warfare strategies.

Support Strategic Communication: Establish official communication tools to refute fake news, present the correct information, and keep people trusting national projects such as CPEC.

Promote Research and Innovation: Pakistan should encourage research in the areas of cyber-security, AI, and information warfare to over the long term come up with solutions that are homegrown and not overly dependent on foreign sources.

Enterprising regional partnership: Build regional cooperation and dialogue as a means of addressing hybrid threats in one, establish a networked solution to information and cyber security in South Asia.

References

Afzaal, M. (2020). The China-Pakistan economic corridor of the Belt and Road Initiative concept, context and assessment: by Siegfried O. Wolf, Switzerland, Springer, 2020, 404 pp., 88, ISBN 978-3-030-16198-9 (Vol. 26, No. 5, pp. 691-695). Routledge.

Ahmed, S. (2024). Asian journal of International Peace and Security (AJIPS) ISSN-e: 2707-8809 Vol. 8, No. 3, (2024, Autumn), 39-57. Asian Journal of International Peace & Security (AJIPS), 8(3), 39-57.

Ali, F., Khan, S. R., & Ullah, F. (2025). Hybrid warfare and non-state actors in the middle east and south asia: emerging threats and strategic responses. Policy Journal of Social Science Review, 3(11), 61-69.

Anwar, U., & Atif, M. (2025). CPEC & BRI regional game changers: security and geopolitical implications in Pakistan. Australian Journal of Maritime & Ocean Affairs, 1-17.

Aslam, H. A. (2025). AI Driven Cyber Warfare Between China and India and Its Impact on Pakistan's National Security. Journal of Regional Studies Review, 4(1), 424-432.

Clarke, M., Small, A., & Keough, J. (2017). China's Belt and Road initiative: Views from along the Silk Road. Asia policy, 24, 65-122.

Clary, C., Lalwani, S., & Siddiqui, N. (2021). Public opinion and crisis behavior in a

Online ISSN 3007-3197
Print ISSN 3007-3189

nuclearized south Asia. International Studies Quarterly, 65(4), 1064-1076.

Farwa, U. (2018). Belt and road initiative and China's strategic culture. Strategic Studies, 38(3), 40-56.

Hoffman, F. G. (2014). Hybrid warfare and challenges. In Strategic studies (pp. 329-337). Routledge.

Hussain, M., & Ahmed, S. (2021). China's Strategic Engagement with Pakistan and its impact on the South Asian Balance of Power. Available at SSRN 4917506.

Kalpokas, I. (2017). Information warfare on social media: A brand management perspective. Baltic Journal of Law & Politics, 10(1), 35.

Khan, K., Uddin, I., & MaghfoorUllah, M. A. (2024). Pak-China Strategic Partnership and Its Impact On Regional Power Structure. ISAR Journal of Arts, Humanities, and Social Sciences, 2(8), 1-9.

Khan, S. U., Shah, I. U., Shah, K., & Iqbal, M. J. (2025). The Role of China-Pakistan Relations in the Global Tech Competition, Especially in Areas like 5G, AI, and Cybersecurity. Review of Education, Administration & Law, 8(1), 73-85.

Kofman, M., & Rojansky, M. (2015). A closer look at Russia's' hybrid war'. Woodrow Wilson International Center for Scholars.

Kuszewska, A., & Nitza-Makowska, A. (2021). Multifaceted aspects of economic corridors in the context of regional security: the China–Pakistan economic corridor as a stabilising and destabilising factor. Journal of Asian Security and International Affairs, 8(2), 218-248.

Maqsood, A. (2025). Leveraging Regional Supply Chains for Strategic Connectivity. Strategic Studies, 45(1), 116-135.

Richelson, J. T. (2018). The US intelligence community. Routledge.

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Profile Books.

Rolland, N. (2017). China's Eurasian century. Political and Strategic Implications of the Belt and Road Initiative, 32-39.

Rolland, N. (2017). China's Eurasian century?: Political and strategic implications of the belt and road initiative. National Bureau of Asian Research.

Saud, A., & Kazim, N. (2022). Disinformation and Propaganda Tactics: Impacts of Indian Information Warfare on Pakistan. Journal of Indian Studies, 8(02), 335-354.

Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Small, A. (2014). The China-Pakistan axis: Asia's new geopolitics. Oxford University Press.

Surahio, M. K., Gu, S., Mahesar, H. A., & Soomro, M. M. (2022). China–Pakistan economic corridor: macro environmental factors and security challenges. Sage Open, 12(1), 21582440221079821.

Ullah, F. (2024). The Impact of Pakistan-China Security Cooperation on South Asia's Security Architecture. Pakistan Review of Social Sciences (PRSS), 5(2), 15–19.

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking (Vol. 27, pp. 1-107). Strasbourg: Council of Europe.

Online ISSN 3007-3197
Print ISSN 3007-3189

Wolf, S. O. (2019). The China-Pakistan Economic Corridor of the Belt and Road Initiative: Concept, Context and Assessment. https://doi.org/10.1007/978-3-030-16198-9

Yamin, T. (2019). HYBRID WARFARE–CHALLENGES FOR PAKISTAN. Strategic Thought, 1, 128-139.

Zhao, X. (2025). Technological hedging and differentiated responses of Southeast Asian countries to US–China technological competition: A case study on artificial intelligence (AI). The Pacific Review, 38(3), 502-533.

Zhao, X. (2025). Technological hedging and differentiated responses of Southeast Asian countries to US–China technological competition: A case study on artificial intelligence (AI). The Pacific Review, 38(3), 502-533.

Zingel, W. P. (2020). Book review: Siegfried O. Wolf: The China-Pakistan Economic Corridor of the Belt and Road Initiative. Concept, Context and Assessment. (Contemporary South Asian Studies). Cham: Springer, 2020. ISBN 978-3-030-16198-9. International Quarterly for Asian Studies (IQAS), 51(1-2), 279-281.