Otoritas : Jurnal Ilmu Pemerintahan Vol. 15, No. 3, 2025
DOI: https://doi.org/10.26618/ojip.v15i3.18100

Governance challenges and non-traditional security threats in Pakistan: terrorism, cybersecurity, and climate risks

Muhammad Bahar Khan[1], Muhammad Khalid Anser[2], Imran Naseem[3], Alamzeb Aamir[4], Khalid Zaman[5*)]

[1]*Department of Pakistan Studies and International Relations, Abbottabad University of Science and Technology, Pakistan*
[2]*Department of Economics, Recep Tayyip Erdoğan University, Türkiye*
[3]*Department of Pakistan Studies and International Relations, Abbottabad University of Science and Technology, Pakistan*
[4]*Department of Management Sciences, FATA University, Pakistan*
[5]*Department of Economics, The University of Haripur, Pakistan*

Abstract

Pakistan's security concerns have expanded to include terrorism, cyber insecurity, and climate-induced risks. These interconnected concerns are straining governance, institutional coordination, and long-term stability, necessitating a comprehensive reevaluation of national security beyond military solutions. The study analyses Pakistan's non-traditional security threats over time, evaluates institutions and governance's responses to cyber threats, climate change, and terrorism, and identifies policy gaps that hinder integrated security management. Systematic document analysis underpins the study's qualitative research design. Official papers, anti-terrorism initiatives, cybersecurity frameworks, climate change adaptation measures, and scientific studies from 2001–2024 provided information. The study uses thematic and comparative methodologies to track risks, institutional responses, and governance effectiveness across sectors. The Result show Three significant patterns emerge. First, even while counterterrorism efforts have considerably reduced militant violence, governance issues, including social and economic marginalization and ideological radicalization, have not been addressed. Second, as Pakistan's digital dependence has outpaced institutional cybersecurity safeguards, regulatory monitoring and policy responses are lacking. Third, climate-related hazards, including water stress and extreme weather events, aggravate food insecurity and rural livelihoods, increasing social and security vulnerabilities. The lack of policy integration and interagency coordination limits long-term effectiveness across the board. The study's results and policy implications suggest that integrated governance is needed to address Pakistan's security issues, rather than sector-specific initiatives. Policy implications include improving institutional coordination, integrating climate resilience and cybersecurity into national security planning, and implementing inclusive governance reforms to promote community resilience. A flexible and comprehensive plan is needed to improve national stability and sustainable growth.

Keywords: *governance, terrorism, cybersecurity, climate risk*

*)Corresponding author
Email: khalid_zaman786@yahoo.com

Introduction

Modern threats transcend military wars; thus, national security studies are becoming more comprehensive. Recent research suggests that transnational militancy, cyber vulnerabilities, climate-induced disruptions, and domestic instability have reshaped the security paradigms of developing countries (Lopes, 2024). Khan's (2025)

research shows how geopolitical conflicts, technology development, and environmental fragility are interconnected. Cyberwarfare and climate change threaten Pakistan and other countries. Security literature has adopted integrated frameworks that combine ecological, political, and technological perspectives as the globe moves from military models to resilience-based national security policies (Pashentsev & Kolotaev, 2025). This study fits into this shifting academic climate by examining Pakistan's internal and cross-border concerns and hybrid and non-traditional security issues, while also extending the discussion toward how these pressures accumulate within governance systems and policy coordination.

Scholarly interest in Pakistan's security situation is rising; however, most research focuses on cyber threats, climate change, and terrorism (Saad et al., 2024). Most past research has focused on counterterrorism without adequately analyzing how modern hazards overlap and reinforce each other (Wahab, 2024; Ullah et al., 2025). Environmental shocks, digital vulnerabilities, and violent extremism affect Pakistan's national security, but little is known about how successfully its policies manage these challenges. Many studies on Pakistan's security have examined terrorism, counterinsurgency, and military-civilian interactions from a national security or conflict studies perspective (Shahzad et al., 2026; Ghalib, 2025). Climate vulnerability and cybersecurity governance have been studied independently as technology or industry-specific issues rather than integrated security challenges (Khan et al., 2025). Thus, previous research has focused on specific risks rather than their interrelation, cumulative governance burden, or institutional coordination effects. Most current research on non-traditional security threats focuses on event-driven or operational analysis, leaving unsolved questions about governance, policy consistency, and institutional resilience.

Another considerable research gap is the conceptual divergence between governance analysis and security studies. The social and economic repercussions of insecurity are usually described rather than analysed in an institutional or policy-focused perspective. In Pakistan, climate-related concerns are mainly discussed in terms of development and the environment, rather than external security or governance (Makki et al., 2025; Yousaf et al., 2025). Cybersecurity research focuses on technology, legislation, and events, seldom discussing cyber threats in the context of national security policy or state capabilities. Terrorism, cyber risks, and climate stress are interrelated; little is known about how they affect governance systems in impoverished or unstable states like Pakistan. This study addresses that requirement by presenting an integrated governance perspective of Pakistan's non-traditional security challenges.

Instead of treating climate change, cybercrime, and terrorism separately, the study examines their interconnection. It then assesses the extent to which these three elements strain state responsiveness, policy coordination, and institutional performance. Using policy documents, strategic plans, and scholarly sources across time, the study reveals how governance structures have altered (or not) to address evolving security demands. This effectively separates the study's goals, i.e., tracking threats and how governments have responded, from its contributions and reorienting Pakistan's security discourse toward adaptable governance, policy coherence, and institutional resilience. Pakistan and other multidimensional security governments may benefit from this approach, which provides a more uniform analytical framework for understanding non-traditional security issues.

Comparing how other nations with similar threat contexts have addressed hybrid security concerns offers a global comparative dimension to the study. Turkey

and Nigeria demonstrate how governments handle terrorism in politically difficult countries, whereas Indonesia and Malaysia demonstrate community-led de-extremization and counter-radicalization. Comparing Pakistan with the UK, Estonia, and Singapore shows that digital governance, cybersecurity architecture, and cybercrime response mechanisms could be improved. The Philippines, Bangladesh, and Nepal are climate-vulnerable countries that serve as models for resilience planning, climate change adaptation, and disaster preparedness. Pakistan's experiences are placed in this global context to identify commonalities and policy breakthroughs that might inform national responses.

Among South Asian countries, Pakistan has a significant strategic location in which internal and external factors and complex security dynamics have been compelling to change its foreign policy directions and values (Khan &Naazer, 2023). In the 21st century, every state is trying to bring new dimensions to improve its economic, security, and trade landscape. The primary aim is to highlight the terrorist threats, emerging cyber warfare challenges, environmental and medical risks, and climatic changes; those are the predictiveness of the significant challenges against medical, agricultural, economic, security, and human survival. This research will delve into these multifaceted expected threats because of their impacts on Pakistan's geography, topography, economic production, global trade ratio, global relations with security, foreign policy direction, and regional unity.

Due to possessing the best geography, Pakistan had been facing terrorism, which reshaped the regional and geopolitical development of this country. During the Afghan-Russian War of 1979-88, the external actors tried their best to develop their secret purpose practically, which they succeeded. After the Afghan-Russian War, Pakistan had to face terrorism for decades (Khan et al., 2024). Keeping view of its security requisites, Pakistani supported Afghan mujahideen against Soviet forces through thick and thin in the shape of warriors. Later, cross-border influence operations named them terrorist organizations like Al-Qaida. The groups that were entered and trained by external actors later tried their best to get involved in Pakistani systems and became severe threats to the security of Pakistan. After the 9/11 incident, a terrorist organization by the name of Tehrik-i-Taliban Pakistan (TTP)" emerged in 2007 and started its terrorist activities to destroy domestic, military, and civilian sites posing to impose Islamic Sharia law all over the country, which caused a de-stable state system. (Khan& Wei, 2016). Another terrorist organization, the Balochistan Liberation Army (BLA), with several other separatist factions, tried to contribute to internal, domestic, administrative, political, financial, linguistic, and ethnic conflicts that had been demanding more autonomous power and topographical resource control.

Terrorism led Pakistan's socio-economic system to destruction. Terroristic attacks caused life, social, and economic loss and created a big gap between the state administrative relations as well as increased misunderstandings among its citizens (Rose, 2009). In the past, the tourism industry was notably affected. On the other side, due to security concerns, foreign investment degraded, and Pakistan faced financial losses. Moreover, terrorism also causes academic and health development, which Pakistan has closely experienced. Under military operations like "Zarb-e-Azb" and "Radd-ul-Fasaad," Pakistan has undertaken several counterterrorism activities, the aim of which was to dismantle the terrorist network and restore social, economic, educational, and trade stability (Irfan et al., 2022). Despite these struggles, Pakistan is facing security challenges. Now, it is necessary to solve comprehensive counter-radicalization programs, effective intelligence-sharing, and address underlying socio-

economic issues that have been and are contributing to religious, regional, and ethnic extremism (Rashid et al., 2023). The digital age is predicting dangerous cyber warfare. This thing is emerging in the shape of significant security threats. Like every state, Pakistan is also increasing its reliance on modern technologies, which is exposing it to serious cyber threats. Most important are state-sponsored attacks, cybercrimes, and hacktivism (Djenna et al., 2021). Adversarial powers aim to use these cyber-attacks in the shape of asymmetric warfare, whose purposes are to de-shape Pakistan's critical infrastructure, disrupt the necessary services, create upsetting, gather intelligence data, and degrade public confidence (Anjum, 2020). The proliferation of cybercrimes, identity theft, and attacks poses further risks to the social, economic, educational, industrial, and trade systems (Mphatheni& Maluleke, 2022).

Highly critical systems, such as networks for communication, electrical power lines, and financial institutions, are seriously threatened by cyberattacks, which could have disastrous effects on both national security and financial wellness (Lehto, 2022). Attacks like this can reveal private data, cause significant financial losses, and interrupt operations. Further aggravating the issue is the public's declining faith in digital systems, which undermines trust in the functioning of the public and private sectors. In the long run, this lack of trust may result in fewer users interacting with websites and applications and a greater susceptibility to online attacks in the future. Strong precautions for cyber security and a greater public understanding are necessary to address these concerns. The National Reaction Centre against Cyber Crime (NR3C) and national cyber security policies have been established by Pakistan in order to strengthen its cyber defenses (Noor et al., 2024). Nonetheless, obstacles, including few resources, specialized expertise requirements, and the quick evolution of cyber threats, demand constant modification and advancement.

Due to its geographic location, extreme temperatures, shortages of water, and destruction of the environment are just a few of the hazards Pakistan is particularly prone to the country's sustainable development agenda. Increasingly frequent flooding, which is exacerbated by glaciers that are melting and heavy monsoon rains, destroys infrastructure extensively, uproots societies, and interferes with farming (Adnan et al., 2024). Frequent droughts hurt agricultural output and accessibility of water, endangering the rural economy and nutritional stability. One of the main problems is the water shortage, which results from excessive extraction, inadequate utilization, and global warming. The water supply decreased in the basin containing the Indus River, which is essential for the agricultural sector, has an impact on crop production and food availability (Janjua et al., 2021). In addition to posing health problems, elevated and scorching temperatures also burden energy supplies and reduce production. Pakistan's reaction is to create national environmental strategies and participate in global accords like the Paris Agreement. It is imperative to implement initiatives like enhanced water management and reforestation efforts. However, execution is complex due to a lack of funding, unstable political environments, and the requirement for solid institutional structures (Hafeez et al., 2020).

The interaction of cyber warfare, climate-related hazards, and terrorism illustrates the complexity of Pakistan’s contemporary security landscape. Climate change–induced disasters can intensify social and economic pressures, potentially increasing the risk of radicalization and violence; for instance, water scarcity in already fragile areas may exacerbate competition over resources, heighten communal tensions, and contribute to broader instability (Ahmed & Shahzad, 2021). At the same time, the nexus between cyber warfare and terrorism further complicates national security:

terrorist organizations may leverage cyber capabilities to enhance operational effectiveness, while state-sponsored cyberattacks could target critical infrastructure in ways that create opportunities for terrorist exploitation and deepen destabilization (Akram et al., 2023). Moreover, as information technologies are increasingly used to manage climate-related data and critical infrastructure systems relevant to disaster risk reduction, cybersecurity becomes integral to mitigating the impacts of climate change–driven hazards and ensuring continuity of essential services during crises (Argyroudis et al., 2022).

Addressing these interlinked risks requires comprehensive, coordinated approaches. First, Pakistan should develop and implement integrative policymaking strategies that explicitly account for the interdependencies among environmental threats, digital conflict, and terrorism. Second, institutional capacity must be strengthened through sustained investment in technological modernization, professional training, and research to enhance the operational readiness of agencies responsible for cyber defense, disaster response, and public safety. Third, international collaboration should be expanded through joint research initiatives, technical assistance exchanges, and intelligence and information-sharing arrangements, given that both climate change and cyber conflict are transnational challenges that demand cooperative solutions. Fourth, community engagement should be prioritized to build local resilience through education programs, public awareness campaigns, and participatory mechanisms that empower communities to prepare for, respond to, and recover from cascading threats.

Pakistan's security environment is increasingly defined by the convergence of established and emerging risks. The combined pressures of cyber warfare, terrorism, and climate change produce a fluid and uncertain threat landscape that necessitates an integrated strategic posture. By coordinating policies across domains, reinforcing institutions, engaging in sustained international cooperation, and cultivating community-level resilience, Pakistan can enhance stability and safety amid these interconnected challenges.

Insurrection and terrorist attacks have always been sources of security concerns for Pakistan. There have always been significant hazards associated with organizations like Tehrik-i-Taliban Pakistan (TTP), Al-Qaeda, and Baloch separatists. In order to confront current and real risks, it is helpful to have an understanding of these hazards in order to establish focused counterintelligence strategies, regulations, and operational approaches. Conventional security risks necessitate using proven defenses and tactics, like intelligence collection and military actions. However, cutting-edge strategies and technical advancements are needed to combat increasing dangers like cyberspace warfare and the impact of climate change. Pakistan must constantly update its cyber security processes and infrastructures to safeguard vital information and computer systems as cyber threats change. Similarly, building infrastructure resistant to climatic impacts and including environmental variables in national security plans are necessary to mitigate dangers brought on by climate change (Hussain et al., 2023). Combining defenses against established and novel hazards is critical to a comprehensive security strategy. This includes preparing for long-term problems like global warming and handling current ones like terrorism. Enhanced water management mechanisms and catastrophe preparedness measures can be implemented to lessen the effects of extreme weather occurrences and, consequently, the likelihood of economic and social problems, volatility, and disputes (Reiter et al., 2022). Security risks directly impact the viability and expansion of the economy. Markets are upset, business

is discouraged, and resources are strained by violence. Environmentally friendly growth must tackle both established and new forms of danger. A low interruption to economic activity is guaranteed when infrastructure is invested to guard against climatic hazards and cyber threats. Furthermore, for a long time, financial advantages and stabilization can be derived from concentrating on environmental sustainability and technical improvements (Abbasi et al., 2022).

The given discussion leads to the following research questions. First, how the dynamics of terrorism and insurgency in Pakistan do intersect with the country's cyber security challenges, and what strategies can be developed to address these intersecting threats? Second, what is the impact of climate-induced risks, such as extreme weather events and resource scarcity, on the socio-political stability of Pakistan, and how do these impacts exacerbate existing security threats like terrorism and cyber-attacks? Third, how do different sectors of Pakistani perceive and respond to the combined threats of terrorism, cyber warfare, and climate change, and how effective are these responses in mitigating the overall security risk?

Since international aspects of developing dangers are common, cooperative strategies are needed. Global collaboration is necessary because cyber dangers and potential hazards from climate change are not limited by borders between states. Pakistan may address these issues more skillfully and support regional and global peace and security by proactively participating in international forums and collaborations (Shah et al., 2024). Pakistan must comprehend established and new security risks to survive and remain stable. To manage current threats and prepare for future difficulties, an extensive plan incorporating cyber security, adaptation to climate change, and counterterrorism tactics is necessary. Thanks to this broad comprehension, Pakistan can bolster its worldwide stature, foster social cohesiveness, assist economic growth, and improve national security. Pakistan can navigate its complicated security environment and secure its prospects for future prosperity and security by tackling these numerous threats.

Research Methods

This qualitative descriptive study examines how climate change, cybercrime, and terrorism are affecting Pakistan’s non-traditional security concerns. A descriptive technique is appropriate for mapping risk dynamics, governance responses, and institutional patterns, not for establishing causal links or predicting quantitative implications. This research carefully tracks policy changes, security trends, and institutional responses to show how various categories of risk shape Pakistan’s present security scene.

Data collection followed a well-defined source-selection method to ensure openness, relevance, and analytical rigour. Secondary sources were identified using the following terms: “national security policy,” “climate security,” “Pakistan security,” “terrorism and insurgency,” “cybercrime Pakistan,” “cybersecurity governance,” and “cybercrime in Pakistan.” The investigation used academic journals, government documents, reports from international organisations, and reputable think tank publications. Policy and institutional materials were sourced from government websites and reputable international organisations, while academic literature was sourced from Scopus, Web of Science, and Google Scholar. It limited its emphasis since Pakistan’s security, digital infrastructure, and climatic vulnerabilities changed significantly between 2014 and 2024.

Pakistan's sources on terrorism, cybersecurity, and climate risk, as well as government responses, were prioritised. Any material with policy analysis, strategic appraisals, or empirical data on national or sectoral security governance was evaluated. Non-peer-reviewed views, journalistic remarks without reputable sources, and documents that did not directly address security or governance were excluded. Information on terrorism was triple-checked against national security databases, military briefings, and reputable news reports; cybersecurity was informed by the National Response Centre for Cyber Crime and national and international cybersecurity assessments; and climate-related risks were examined with the IPCC, FAO, national disaster management authorities, and regional climate studies. This method enhanced sector-specific accuracy.

Analytical methods included a thematic and comparative evaluation of selected resources. The materials were coded and organised under topics including risks, institutions, policies, government coordination, and sector interactions. Policy reviews examined the flexibility, breadth, and coherence of current security systems across these three domains. Next, the study conducted a comparative analysis to identify governance responses that were comparable or dissimilar, highlighting areas of coordination gaps or institutional fragmentation that hindered long-term security efforts. This systematic analytical process ensures evidence-based, coherent, and goal-centred research findings.

Realist Theory of International Relations

The realistic theory of international relations (IR) highlights the global system's chaotic structure and the crucial roles played by government authority and national interest. It asserts that states function as self-help organizations with security and power as their main priorities. Realistic people contend that because there is no single governing body in the framework of international relations, nations must rely on their resources to maintain and grow their positions of authority. Realist analysis of Pakistani terrorism can be done by looking at it through the prisms of safety issues and authority from the state. A variety of internal and external reasons that undermine the integrity of states and independence can give rise to terrorist organizations. The power and geographical sovereignty of the Pakistani state, for example, may be threatened by the emergence of organizations such as Tehrik-i-Taliban Pakistan (TTP). The government's reactions to terrorism are explained by the theory of reality, which emphasizes martial and safety measures meant to maintain national power and peace (Mahmood, 2022). Reality is also essential in comprehending Pakistan's border conflicts, especially with India. Powerful and influential struggles can be observed in the ongoing conflict around Kashmir and other territorial disputes. Realist theory clarifies that the need for an advantageous strategic position and to maintain a power balance fuels these border conflicts. For instance, both nations' defense plans and military postures show their efforts to protect their interests and preserve their control in the area (Budiana et al., 2023). Realist philosophy emphasizes how crucial it is to strengthen military might and mutually beneficial relationships to counter conventional security concerns. The Pakistani government's strategies have centered on strengthening defenses, carrying out counterterrorism efforts, and pursuing diplomatic measures to resolve disputes in the face of terrorism and border concerns. The country's defense tactics, especially its strategy regarding regional alliances and military modernization, are informed by the realism focus on the relationship between power and national interest (Kuszewska& Nitza-Makowska, 2021).

Securitization Theory

The Copenhagen School of Security Studies created the Securitization Theory, which focuses on how problems are portrayed and put together as security risks. This theory states that securitization entails a procedure in which problems are framed as imminent dangers, necessitating extraordinary actions and resources above and beyond the scope of conventional politics (Nyman, 2023). The three leading players in this procedure are the audience, the referring object, and the securitizing actor. The development of securitization is significantly hampered by cyber warfare. Cyber attacks have grown in frequency as technology has developed. Cyber warfare must be framed as a danger to vital facilities, national security, and financial stability to be considered a security concern. Hacks that go after Pakistan's power networks or banking establishments, for instance, are presented as existential dangers that need solid cyber security defenses and cross-border collaboration. Establishing organizations such as the National Response Centre for Cyber Crime (NR3C) and developing national cyber security rules are examples of how cyber warfare is becoming more securitized. Risks brought on by climate change, like severe weather and water shortages, are being presented increasingly as security concerns. Understanding how environmental modifications affect the stability of society, economic growth, and national security is necessary to securitize climate threats. For example, persistent droughts and flooding are presented as risks to community cohesiveness and food security, requiring coordinated approaches to disaster preparedness and adaptation to climate change. Pakistan's involvement in international environmental accords and the development of national climate policies indicate the securitization of climate change risks (Chaudhry, 2022). Particular regulations and reaction mechanisms have been developed due to the securitization of new hazards, such as technological warfare and climate issues. Improvements in technological advances, training, and international collaborations are all part of the strategy for cyber dangers. Encouraging disaster readiness, including environmental factors in national security plans, and implementing adaptation measures are all necessary to mitigate climate hazards.

Human Security Framework

The emphasis has shifted from state-centric to individual-centric safety in the human safety system. It strongly emphasizes autonomy and safeguarding by tackling risks to individual security, general well-being, and honor. Financial, nutrition, medical care, ecological, and family safety are only a few topics covered by this structure. One of the most critical components of security for humans is financial safety, including work, resource availability, and economic sustainability. Financial risks affect the survival and well-being of Pakistan and are made worse by terrorism, cyberattacks, and climate change (Ahmad & Jahangir, 2023). In order to tackle fiscal stability, policies that support financial stability, creation of employment, and growth in the economy must be put into place (Al-Saadi &Khudari, 2024). A vital part of humanity's safety is food security and health security. Risks brought on by climate change, such as severe weather and water scarcity, can impact food access and agricultural output. Furthermore, access to health care and healthcare systems might be disrupted by terrorism and conflict. Integrated approaches to tackle the impact of the environment, fortify the healthcare system, and improve access to critical services are needed to ensure food and medical security). Protection against abuse, assault, and human rights violations is all included in the safety. The safety of individuals is threatened in Pakistan by terrorism, disputes, and socioeconomic upheaval. In order to ensure people's safety, it is necessary to

uphold human rights, bolster security forces, and deal with the fundamental reasons for violence and disputes (Akram & Tariq, 2024). Regulations and tactics that put the welfare of people first and deal with unconventional dangers are influenced by the Universal Security Agenda. This entails implementing social protection initiatives, improving healthcare provisions, and advancing human rights. This paradigm emphasizes the necessity of comprehensive strategies for Pakistan that prioritize the safety and empowerment of persons while addressing the interconnectedness of security concerns (Hussain & Bhatti, 2024).

Results and Discussion

The research found that terrorism, cyber vulnerabilities, and climate-induced threats contribute to Pakistan's hazardous environment. Pakistan has made considerable achievements in counterterrorism, notably after Zarb-e-Azb and Radd-ul-Fasaad, but empirical research shows structural problems remain prevalent. Due to chronic radicalization, social marginalization, and institutional deficiencies, extremist groups might restructure in unexpected ways. The study's findings support Rehman et al. (2025) and Kashif et al. (2025) 's claims that Pakistani terrorist networks exploit governance vulnerabilities and react quickly to governmental pressure. The study found that cyber vulnerabilities and environmental stress exacerbate conventional threats in Pakistan's security situation, providing a more complete picture than studies that focus solely on terrorism. Pakistan is seeing increasing cyberattacks, including financial crimes, critical infrastructure breaches, digital espionage, and misinformation operations. Despite initiatives such as the National Response Centre for Cyber Crime, institutional capacity, legal frameworks, and technical preparedness, these cannot confront modern cyberwarfare. These findings are consistent with global cybersecurity assessments, such as those by Ali et al (2025), which show that developing-world nations with less digital governance expertise are more vulnerable to cyberattacks. The study shows that cyber threats, political decision-making, and social vulnerabilities are interrelated, contrary to earlier studies that focused on technology (Adeyeri&Abroshan, 2024; Dekker &Alevizos, 2024). This research shows how cyber insecurity exacerbates national security challenges, including online radicalization, disinformation, and cross-border influence operations.

Climate-related data support the view that floods, droughts, heatwaves, and other severe weather events threaten human security and the Pakistani government (Usman et al., 2025). Due to their devastating effects on rural livelihoods, food security, and internal displacement, climate-related disasters create societal unrest and grievance-based violence. Environmental shocks intensify conflicts and strain government institutions in countries like the Philippines, Bangladesh, and Sudan. This study demonstrates that climatic vulnerability in Pakistan interacts with terrorism and governance limits. This is more comprehensive than past Pakistani climate assessments, which frequently separate environmental concerns from national security threats (Abbas et al., 2024). Comparing these data with the global literature reveals both parallels and differences. Pakistan, like Nigeria and Indonesia, has mixed problems of terrorism, inadequate governance, and socioeconomic disparity. Cyber governance is better in the UK, Singapore, and Estonia than in Pakistan. Pakistan is more climate-vulnerable than middle-income countries with superior adaptation mechanisms, underscoring the crucial role of institutional resilience as a differential. These comparisons place Pakistan's security problems in the context of global trends and indicate whether the country aligns with or deviates from theoretical assumptions.

Table 1 shows the main climate-related events and their impacts on Pakistan's economy for the period 2001 to 2025.

Table 1. Major Climate Related Events and Impacts in Pakistan (2001–2025)

Year / Event	Type of Event	Key Impact Indicators
2001 Islamabad Cloud Burst	Extreme rainfall	~620 mm in 24 hours; ~61 fatalities; urban flash floods
2010 Pakistan Floods	Monsoon floods	Affected ~20 million people; ~$10 billion in economic losses
2011 Sindh Floods	Monsoon flooding	~434 fatalities; ~5.3 million affected; ~6.79 million acres inundated
2015 Heatwave & Tornado	Heatwave/tornado	~1,200+ heatwave deaths; windstorm fatalities ~45
2022 Pakistan Mega-Floods	Monsoon floods	~1,739 deaths; ~33 million affected; ~$30–40 billion losses; major infrastructure & agricultural damage
2022 Murree Snowstorm	Snowstorm	~23 casualties
2025 Extreme Heat & Glacial Melt Floods	Heatwave + flash floods	Temperatures ~48.5°C; ~72 deaths; rapid glacial melt
2025 Monsoon-related Rains	Monsoon flooding	~178+ deaths; 82% increase in July rainfall vs 2024

Source: FAO (2023); IPCC (2022); and Balcoh (2025).

From the early 2000s to the present, Pakistan has experienced urban flash floods, record monsoon flooding, and extreme heatwaves. Climate shocks created socio-economic hardship in the 2022 mega-floods, which affected 33 million people and cost $40 billion. These events compound governance challenges and may combine with other security threats, such as displacement, resource conflicts, and infrastructure strain, to strain institutional capacity and public order systems, reducing agricultural productivity, infrastructure, and livelihoods.

The investigation finds that one-dimensional models fail to capture the complexity of Pakistan's security. The hazard matrix is complex and ever-changing, encompassing terrorism, cyberwarfare, and climate change. The results support prior findings and shed light on the interconnectedness of modern security threats. The study expands on previous findings by advocating for multi-sectoral counterterrorism, digital governance, and climate resilience in Pakistan's security policies. This combined approach explains the study's unique scientific contribution and guides policymakers who desire to maintain national stability in an increasingly unstable international context. The following are the key findings of the study, i.e.,

Effectiveness of Current Policies

Pakistan's current safety and security safeguards have produced mixed results, largely because progress has been uneven across different threat areas. Counterterrorism operations such as Operation Zarb e Azb and Operation Radd ul Fasaad reduced many conventional violent threats, but they did not fully resolve deeper problems like the ideological drivers of extremism, gaps in intelligence sharing, and the need for stronger coordination across agencies. At the same time, Pakistan has expanded its cyber security posture through bodies like the NR3C and policy initiatives such as the National Cyber Security Policy, yet rapid technological change, capacity limits, and resource constraints continue to expose vulnerabilities that are difficult to manage with fragmented responses.

These governance and capacity pressures are also visible in Pakistan's climate security experience, where repeated disasters show how environmental instability can overwhelm institutions and compound other risks. The trajectory is clear: the 2001 Islamabad cloudburst caused deadly flash floods, the 2010 nationwide floods affected nearly 20 million people and led to about 10 billion dollars in losses, and severe monsoon flooding struck Sindh again in 2011. Extreme heatwaves and storms followed in 2015, and the 2022 floods marked a turning point by submerging roughly one third of the country, killing more than 1,700 people, affecting 33 million citizens, and creating estimated losses of 30 to 40 billion dollars. By 2025, extreme temperatures reaching 48.5°C accelerated glacier melt and triggered flash floods and landslides, while intensified monsoon rainfall rose by nearly 80 percent in some regions compared to 2024, reinforcing how climate shocks are becoming more frequent and disruptive.

Because these threats overlap, long-term stability depends on moving from tactical success toward an integrated national resilience strategy that connects counterterrorism, cyber protection, and climate adaptation. This requires stronger governance, evidence-based planning, and continuous policy assessment so security frameworks can adjust as conditions change (Javaid, 2022; Kioskli et al., 2025; Adi & Arijanti, 2025). Practical priorities include investment in digital threat monitoring, climate-resilient infrastructure, and institutional capacity to improve responsiveness and reduce systemic vulnerability (Mashwama & Phesa, 2025). Given the cross-border nature of terrorism, cybercrime, and climate impacts, regional and global cooperation is essential for intelligence, technology, and resource sharing (Radanliev, 2025; Park, 2026), while domestically, community engagement and public awareness can strengthen trust and resilience through education on climate risks, online safety, and social cohesion (Ong'esa & Muoka, 2025).

Discussion

During the past couple of decades, there has been a significant evolution in Pakistani terrorism. Pakistan's current terrorism has its origins in the Soviet invasion of Afghanistan in the 1980s, which gave rise to several extremist organizations. Pakistan's safety atmosphere was impacted by the ideology that characterized sure of the Afghan mujahideen, who were supported by the United States and its allies in their struggle against the Russian army. Different terrorist groups, including Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM), came into being in the 1990s and early 2000s. After beginning to concentrate on the Kashmir dispute, these organizations grew and carried out well-publicized assaults both inside and outside of Pakistan. A new era began with the formation of Tehrik-e-Taliban Pakistan (TTP) in 2007. TTP attacks were directed towards both civilian and military installations, and the group's main goal was to enforce an uncompromising understanding of Islamic law known as Sharia. There has already been an enormous impact of terrorism on Pakistan. In terms of the economy, the repeated attacks have taxed resources, disturbed markets, and discouraged foreign investment (Bilal et al., 2022). Terrorism has caused a great deal of death and community uprooting on a social level. There has also been a significant psychological effect on the populace, involving trauma and terror. The emphasis placed by the security services on combating terrorism has taken funds away from other vital sectors like educational and healthcare services, which has made social and economic issues worse. Pakistan has adopted several counterterrorism initiatives in reaction to terrorism. In order to destroy terrorist networks and bring security back to the impacted areas, two significant operations were "Zarb-e-Azb" (2014) and "Radd-ul-Fasaad" (2017)

(Sultan et al., 2024). Even though some of these procedures have been achieved, difficulties still exist. Reducing the impact of terrorism requires effective counter-radicalization initiatives, enhanced sharing of information, and attention to fundamental financial and social issues (Syahputra& Hamid, 2024). Geopolitical competitions and disputes over history are the leading causes of border instability in Pakistan. One of the most divisive problems following the 1947 division of British India was the case of Kashmir, which led to the establishment of the countries of India and Pakistan. Tensions were further cemented by the Indo-Pakistani Wars of 1947–48, 1965, and 1971, frequently made worse by regional and nationalistic disputes (Gillani, 2023). With intermittent clashes occurring along the Joint Working Boundary as well as the Line of Control (LoC) in Kashmir, bordering hostilities between Indian and Pakistani forces have stayed high in recent years. The fragile state of stability in the immediate vicinity was brought to light by the 2019 Pulwama assault and the accompanying Balakot airstrike. Relations are still strained, and stability is being threatened by breaches of peacekeeping and terrorist activity that crosses borders. For the peace and security of the vicinity, the persistent border conflicts have serious consequences.

Pakistan is not a unique contributor to the global trend of cyber warfare as, a severe concern. Cyber attack susceptibility has risen due to the quick digitization of vital services and infrastructure. Attacks on governmental database servers, electricity networks, and financial organizations have recently become more complex. One notable event is the 2018 attack on the National Database and Registration Authority (NADRA) infrastructure in Pakistan, which exposed millions of people's private information (Tahir et al., 2019). Tensions between countries have also sparked cyber activity, with competing states' state-sponsored actors aiming their weapons at Pakistan's computer network. Pakistan has a wide range of internet vulnerabilities. The most critical infrastructure in the nation, such as the power and transport industries, needs to be updated, and there are inadequate defenses against cyber attacks. These security holes result from insufficient employee education and sophisticated cybersecurity safeguards (Bokhari, 2023). Furthermore, the creation of thorough cyber security regulations needs to catch up to the quick growth of technology and connectivity to the internet. Pakistan has made many efforts to strengthen its cyber security stance as a reaction to the increasing threats of technological warfare. A significant effort was made in 2016 to counter cyber threats, creating the National Response Centre for Cyber Crime (NR3C) (Haq&Zarkoon, 2023). To strengthen the nation's cyber defenses, the National Cyber Security Policy of 2021 calls for greater global collaboration, better rules, and more financing for cyber security projects (Akram& Malik, 2023). Notwithstanding, there are still obstacles to overcome, such as the requirement for more resilient deployment and ongoing adjustment to changing threats from cyberspace scenarios.

Data on terrorism shows the extent and trend of militant violence. Pakistan had 971 terrorism-related deaths in 2022, 1,513 in 2023, and 2,236 in 2024. Most occurrences occurred in Khyber Pakhtunkhwa and Balochistan (SATP, 2025). Civilians, security personnel, and rebels have died less since 2014; however, alterations in operational dynamics and the militant revival cause year-to-year variation. SATP records show that battle intensity changes with time, with 7,341 casualties in 2010, 228 in 2019, and 2,927 in 2024 (SATP, 2025). These figures show a general drop from early peaks, but a recent return to violence, allowing an impartial evaluation of Zarb-e-Azb and Radd-ul-Asaad.

Cyber threats in Pakistan have also increased. According to official Parliament numbers, the National Cyber Crime Investigation Agency (NCIA) received 1,955 formal cases and 26,036 inquiries in 2025, indicating a rise in public reporting and cyberspace enforcement issues. The Federal Investigation Agency (FIA) received over 73,000 cybercrime reports in 2024, including financial fraud and data theft, further evidence of cyber vulnerabilities and the financial impact of digital crime (Hussain, 2025). The sheer quantity of complaints shows the significance of cybersecurity risks to individuals, corporations, and government institutions, even without precise economic cost estimates.

Climate-induced environmental issues have visible effects. The 2022 Pakistan floods affected 33 million people, displaced nearly 8 million, and caused $15.2 billion in economic losses and damages, according to the government's Post-Disaster Needs Assessment (PDNA) and UNDP reporting. National and international evaluations support this information (PDNA, 2022). Ndma (2025) reports approximately 1,985 fatalities and tens of millions of people affected by the 2010 floods. The 2025 monsoon season resulted in over 1,000 deaths and severe infrastructure damage in Khyber Pakhtunkhwa and Sindh. Human and economic losses from these floods are high. Rising mean annual temperatures and irregular monsoons are rendering Pakistan increasingly susceptible in several locations.

The safety of Pakistan is seriously threatened by climate change as the nation is highly susceptible to climatic fluctuations. Increased frequency and catastrophic flooding have been caused by increased temperatures and unpredictable weather patterns, especially in the Punjab and Sindh regions. The Himalayan glaciers are melting, which raises river levels and increases the risk of flooding (Nie et al., 2021). Pakistan also has frequent droughts, which affect the availability of water and the productivity of agriculture. Due to altered precipitation patterns and excessive extraction, the Indus Basin—essential to the nation's agriculture—is seeing a decrease in water flow. In addition to uprooting populations and endangering the availability of food, these modifications to the environment also exacerbate economic volatility. One major problem made worse by global warming is the lack of resources. The Indus River system has been experiencing reduced flow due to the combined upstream water consumption and climate variables, making the lack of water especially severe (Mehboob& Kim, 2021). There is more rivalry for a few water resources, which has raised tensions in the immediate vicinity and the possibility of violence over sharing water sources. Pakistan has launched several programs to mitigate the effects of global warming. Reforestation initiatives, better water leadership, and disaster readiness are only a few of the adaptation tactics highlighted in the National Climate Change Policy 2012 and its subsequent amendments. To secure funding and assistance for coping with climate change, the government has also participated in global climate agreements such as the Paris Agreement (Ahmad et al., 2023). Despite these efforts, implementation obstacles such as budgetary limitations, unstable political environments, and the requirement for stronger institutional structures still exist. In order to address these concerns, there has to be greater community participation in resilience to climate change efforts, more financing, and greater collaboration amongst government departments.

Terrorism, cybercrime, and climate change have grown together in Pakistan's security environment during the previous decade. Environmental stress from droughts, water shortages, and agricultural disturbances in Balochistan and Sindh has boosted social instability and terrorist assaults (Bugti, 2025). Extremist organizations exploit

community grievances caused by economic downturns and environmental catastrophes. Extreme droughts and reduced agricultural productivity in southern Pakistan have increased insurgent activity, demonstrating the link between climate and radicalization in vulnerable socioeconomic conditions (Muzamil et al., 2025). This supports the human security framework's key claim that environmental threats may increase conventional security concerns by weakening livelihoods and government capabilities (Siloko, 2024).

Evidence links cyber risks to terrorism. Pakistani terrorist organizations are increasingly exploiting the internet to recruit, distribute propaganda, and plot smaller-scale attacks (Kidwai, 2022). Banned extremist organizations utilize encrypted messaging applications, social media, and forums to recruit, spread ideology, and organize logistics across national and provincial boundaries (Akram & Safdar, 2025). The National Response Centre for Cyber Crime (NR3C) has recorded various cyber-enabled terrorist activities, from phishing attacks on government officials to extremist propaganda online (Stoddart, 2022). These examples reveal the link to cyberterrorism and how extremists might exploit digital flaws to expand their operations.

As more climate monitoring and disaster management systems in Pakistan are digitalized, climate-cyber research is growing. Pakistan's flood early-warning systems, water management platforms, and meteorological data repositories are vulnerable to cyberattacks as their digital infrastructure grows (Ahmed et al., 2025). Breach may impede climate adaptation and disaster response capabilities. If regional flood monitoring systems are broken, warnings will be delayed, and emergency services will be less coordinated, worsening the humanitarian impact of climate-induced catastrophes. By integrating cybersecurity into climate risk management, policymakers can mitigate these vulnerabilities and ensure the nation's digital infrastructure is protected against environmental shocks. This tripartite assessment of climate change, cybercrime, and terrorism in Pakistan shows that all three are linked, underscoring the need for multi-sector security policies.

Evaluation of Existing Security Policies

While evaluating Pakistan's security policies, a thorough analysis of current tactics for dealing with both established and emerging threats is necessary. Guided by current research and recent developments, this discussion highlights the strengths of key regulations and practices while also identifying major shortcomings. Pakistan has implemented a range of counterterrorism measures in response to threats posed by groups such as Al-Qaeda and Tehrik-i-Taliban Pakistan (TTP), including large-scale military operations such as Operation Zarb-e-Azb (2014–2017) and Operation Radd-ul-Fasaad (2017–present). Operation Zarb-e-Azb was designed to dismantle terrorist sanctuaries in North Waziristan and is widely viewed as a decisive intervention during a period of heightened insecurity, producing notable outcomes by degrading militant capacity and restoring state control in affected areas. However, these gains were not sustained evenly across the country, as several groups adapted by shifting organizational structures and tactics, enabling continued activity despite territorial losses (Hussain et al., 2020). Building on these efforts, Operation Radd-ul-Fasaad has aimed to eliminate residual threats and consolidate earlier gains, with evidence suggesting it has helped reduce localized insurgent activity and strengthen internal security across Pakistan (Ali, 2019). Even so, persistent challenges—especially the spread of extremist ideology and weak intelligence coordination across agencies—continue to limit the long-term effectiveness of counterterrorism initiatives (Rahman et

al., 2023). Alongside internal security efforts, Pakistan maintains a heavy military presence along the Line of Control (LoC) with India to deter and respond to cross-border incursions; while this posture has helped prevent large-scale wars, it has not resolved underlying disputes or tensions. Diplomatic efforts such as the Shimla Agreement (1972) and subsequent bilateral engagements have sought to manage border issues, yet recurring clashes and diplomatic breakdowns suggest dialogue alone has not produced lasting stability.

At the same time, Pakistan has expanded institutional and regulatory capacity to address emerging threats, particularly in cyberspace, recognizing cybersecurity as strategically important. The National Response Centre for Cyber Crime (NR3C), established under the Ministry of Interior, investigates cybercrime, supports law enforcement coordination, and carries out public awareness efforts (NR3C, 2023). This institutional approach is complemented by the National Cyber Security Policy (NCSP, 2021), which aims to strengthen cyber resilience, protect critical infrastructure, promote public–private partnerships, and support international cooperation. Despite these steps, implementation remains partial and uneven, constrained by limited resources, insufficient technical expertise within intelligence and law enforcement bodies, and gaps in funding needed to maintain critical digital infrastructure. Although the Prevention of Electronic Crimes Act (PECA, 2016) provides legal penalties, it often fails to keep pace with evolving risks such as cross-border cyberattacks, critical infrastructure intrusions, and ransomware. While NR3C performance indicators point to improvements in response and coordination, the broader institutional posture remains largely reactive rather than proactive, and cyber risks continue to evolve faster than policy and capability development. Addressing these gaps requires sustained investment in technical expertise, legal updates that match current threat patterns, and more effective collaboration between public and private sectors to meet the NCSP's strategic goals.

Beyond terrorism and cyber risks, climate change has increasingly shaped Pakistan's security and resilience environment. Pakistan has signaled commitment to global climate action through participation in international agreements such as the Paris Agreement, which has helped influence domestic priorities for ecosystem protection and emissions reduction. National policy instruments—including the National Climate Policy (2012) and the Climate Change Framework (2014)—were developed to support sustainable development and improve resilience to climate-related impacts (Mumtaz, 2018). Nevertheless, effective implementation has repeatedly been limited by financial constraints and political instability, weakening continuity, enforcement, and long-term programme delivery. These challenges reflect broader policy gaps across Pakistan's security environment. Despite operational progress in counterterrorism, structural and societal weaknesses undermine durable outcomes, particularly because responses have often focused on kinetic measures while giving less attention to the ideological foundations of extremism. Limited community-level engagement and underdeveloped counter-radicalization programming weaken prevention efforts, reduce the durability of stability, and leave space for renewed recruitment over time. In addition, weak or inconsistent intelligence-sharing arrangements across security agencies reduce effectiveness, since anticipating and disrupting threats depends on systematic interagency coordination and timely information exchange. Similar limitations appear in cybersecurity, where rapidly evolving threats outpace defensive capacity, and resource shortages restrict investment in advanced tools and specialized human capital, affecting operational capability in

institutions such as NR3C. Low public awareness and limited digital literacy also remain significant vulnerabilities, indicating a need for more robust education and outreach so safer online behavior becomes widespread and shared responsibility becomes realistic. Climate policy faces parallel problems: political instability and budget constraints often delay or underfund mitigation and adaptation measures, and climate strategies are not consistently integrated into broader national development planning, leading to fragmented priorities, inefficient resource allocation, and missed opportunities to strengthen resilience and sustainable growth. More generally, Pakistan's security policy landscape can appear fragmented, with limited cross-sector coordination producing duplication, gaps in coverage, and reduced effectiveness against interconnected conventional and non-traditional threats. Compounding this is an ongoing tendency to manage symptoms rather than root causes, as underlying drivers—such as socioeconomic marginalization, governance gaps, and structural inequality—can sustain radicalization pressures and broader instability. Overall, Pakistan's security strategies show meaningful strengths alongside persistent limitations in managing terrorism, cyber threats, and climate-related pressures, suggesting the need for a more coherent approach that strengthens interagency information-sharing, invests in technology and human capacity, improves climate implementation, and aligns policies across sectors and institutions.

To enhance security resilience, Pakistan must adopt a multi-pronged strategy that addresses both long-standing and emerging threats through policy reform, cross-border cooperation, technological strengthening, and sustained public education, while also anticipating implementation barriers and practical ways to address them. A central priority is developing and delivering comprehensive counter-radicalization programmes that directly address extremist ideology by promoting moderate narratives, engaging community leaders, and expanding vocational and educational opportunities for at-risk youth (Babur & Noor, 2023). This should be matched by stronger coordination among national security agencies through improved information-sharing channels and the development of a centralized intelligence mechanism to enable rapid collaboration in decision-making and timely dissemination of threat information (Khattak & Asghar, 2024). Border management should also be strengthened through technology-oriented surveillance and control measures, combined with practical cooperation with neighboring states where possible to support effective monitoring of cross-border activity (Kniep et al., 2024). In cybersecurity, Pakistan should expand the National Cyber Security Policy into a comprehensive National Cyber Security Strategy that prioritizes investment in advanced technologies, strengthens critical infrastructure protection, and operationalizes a coordinated national cyber defense plan (Yongmei & Afzal, 2023). Public–private partnerships should be formalized to build capacity through shared best practices, joint simulation exercises, and collaborative development of safeguards against sophisticated cyberattacks (Haque et al., 2023). At the same time, long-term resilience depends on education and workforce development, including expanded training programmes, specialized upskilling for IT professionals, and the integration of cybersecurity competencies into academic curricula (Alnajim et al., 2023).

Climate adaptation efforts should be strengthened through sector-specific planning that addresses how rising temperatures and climate hazards affect infrastructure, agriculture, and water security, with disaster preparedness, resource management, and community-level adaptability built into these plans (Medellín-Azuara et al., 2024). Environmental regulations should be tightened and enforcement improved to reduce deforestation, environmental degradation, and unsustainable water use

(Imran et al., 2024). Pakistan should also encourage investment in renewable energy and green technologies to reduce reliance on fossil fuels and limit climate impacts, including incentives that support research and innovation in clean energy development (Song et al., 2023). Internationally, Pakistan can strengthen its ability to manage transnational threats by deepening regional cooperation with neighboring states and relevant regional bodies, while also engaging more actively in multilateral forums that address security and environmental risks and encourage alignment with international norms and shared best practices (Chou et al., 2024). This external approach should include stronger bilateral agreements with key partners covering cybersecurity, climate mitigation, and counterterrorism, with clear provisions for joint initiatives, structured information-sharing, and reciprocal support. Pakistan should also expand its engagement with global climate programmes and international financing mechanisms to fund national adaptation priorities and develop mitigation and resilience projects with multilateral institutions and international organizations (Belmin et al., 2023).

Modernizing defense and security capability also requires sustained investment in advanced technologies that improve readiness against evolving threats, including unmanned aerial systems, cybersecurity tools, and upgraded surveillance and monitoring systems, supported by targeted infrastructure upgrades and strategic acquisition partnerships (Vajravelu et al., 2023). Building intelligent networks across critical sectors such as communications, transport, and energy can further improve national resilience by enabling faster detection, more efficient response, and better-informed decisions, achieved through the integration of sensors, automation, and data analytics (Wang et al., 2023). Supporting this technological direction requires stronger research and development capacity through increased funding and targeted support for universities and research institutes producing evidence-based solutions to security and resilience challenges (Tula et al., 2023). A stronger innovation culture can also be encouraged through public–private collaboration, competitive grants, and strategic support for start-ups developing security-related technologies to help move innovations into scalable practice (Shah, 2020). Finally, sustained community-based engagement remains essential, including public education initiatives on cybersecurity, climate risks, and counterterrorism to build risk awareness and encourage meaningful participation in prevention and preparedness (Ashraf et al., 2023). Regional resilience programmes can further strengthen local capacity through community responder teams, local preparedness coordinators, and improved partnerships between law enforcement and community stakeholders to support trusted and coordinated responses (Elkhidir et al., 2023). Integrating security themes such as cybersecurity, disaster preparedness, and social cohesion into school curricula can improve awareness among young people (Fuentes, 2023), while structured training and professional development for teachers, public officials, and community leaders can strengthen practical competencies in safety governance, risk communication, and resilience planning (Fu & Zhang, 2024). Taken together, Pakistan's path to stronger security resilience depends on an integrated approach that combines policy reform, international and regional collaboration, technological modernization, research investment, and sustained public education, alongside practical steps to overcome constraints such as limited resources, political instability, technology gaps, and public resistance. By addressing these issues systematically, Pakistan can strengthen its security framework and improve its ability to withstand complex and rapidly evolving threats.

Conclusion

Pakistan's security landscape is becoming more intricate due to the combination of threats brought on by climate change, cyber warfare, and terrorism. First, the study aimed to explore the resolution of Pakistan's cybersecurity issues and the interplay between insurgency and terrorism. Results indicate that cyber risks and terrorism are becoming more intertwined as Pakistani terrorist organizations use digital platforms for recruiting, propaganda, and operational coordination. The National Cyber Security Policy and the National Response Centre for Cyber Crime (NR3C) have established institutional structures to detect, investigate, and respond to cyber events. Despite increased capacity, there is a deficiency in proactive monitoring, financial resources, and technological expertise. The rapid escalation of cyber threats exceeds institutional readiness, requiring upgrades to technological infrastructure and staff skills. It is becoming apparent that cyber defense and counterterrorism must be integrated to mitigate overlapping security challenges.

The second line of inquiry explored the impact of climate-related calamities, such as droughts and floods, on Pakistan's social and political stability, as well as their contribution to security challenges, including cyberattacks and terrorism. The results indicate that climate-related disasters, such as the mega-floods of 2010 and 2022, heatwaves, and water shortages, have strained governmental institutions and critical infrastructure. Environmental shocks amplify extremist influence and cyber exploitation by inducing population relocation, service disruptions, and resource competition, so indirectly impacting security. Historical climate data indicate that disaster management and national security policies must include climate resilience, given rainfall patterns, flood-related fatalities, and economic losses.

The third inquiry is to investigate Pakistani society's attitudes and reactions towards terrorism, cyberwarfare, and climate change to determine whether these responses mitigate security threats. Research indicates that the government and military possess cyber threat and terrorism strategies. Nonetheless, insufficient transparency, funding, and collaboration between the public and private sectors, particularly between local communities and enterprises, hinder the effectiveness of resilience programs. Long-term security and resilience need preparedness and social cohesiveness. Public awareness campaigns, community education programs, and partnerships between the state and civil society have enhanced these traits.

To enhance national security, policymakers should augment coordination among government entities, improve technological proficiency, and raise financial and human resource allocations. Counterterrorism and cybersecurity strategies must include resilience to catastrophes and climate adaptation to mitigate vulnerability to environmental shocks. Enhanced public awareness initiatives and community involvement are essential for fostering societal resilience and institutional backing. Collaboration at both regional and international levels is essential for exchanging knowledge, technology, and best practices to address transboundary cyber threats and security issues arising from climate change.

The National Counter Terrorism Authority (NACTA) should be a primary focus in the fight against terrorism and extremism. Over the following year, it should steadily increase federal-provincial coordination in this area. Data-sharing between intelligence agencies, standardizing community involvement initiatives to combat violent extremism, and establishing quantitative metrics to measure intervention outcomes, such as decreases in recruitment rates and terrorist incidents, is crucial. Cybersecurity goals should include public-private partnerships to strengthen cyber defenses across

banking, energy, and transportation, as well as expanding the National Response Centre for Cyber Crime's operational capabilities and technology infrastructure. A 24-month implementation timeframe, with criteria including incident response time, cyberattack mitigation, and training for government and commercial-sector personnel, is needed. Climate resilience initiatives should work with provincial and national disaster management agencies to install early warning systems, modify infrastructure, and launch community-level adaptation programs in flood- and drought-prone areas. Methodically calculating costs and resource needs using predicted climate risk models and flood damage assessments enables realistic, focused funding allocation. To evaluate reforms and drive policy changes, quantitative and qualitative performance indicators should be attached. Implementing monitoring and evaluation mechanisms across all areas is essential. This strategy acknowledges the political and bureaucratic complexity of multi-sectoral change and bridges analytical diagnosis and practical prescriptive action by identifying roles, deadlines, and tasks.

The study has several limitations due to its qualitative nature. It uses secondary sources such as academic papers, government reports, and policy documents that provide policy and historical context, but do not address operational efficacy or local security risk perception. Government officials, cybersecurity professionals, and community members have inadequately reflected opinions due to a scarcity of source data. Subsequent studies need to include surveys, interviews, or focus groups to evaluate attitudes, preparation, and treatment efficacy. Investigating South Asian nations may facilitate the management of terrorism, cyber threats, and climate change challenges. Quantitative assessments of the social and economic implications of climate change, cybercrime, and terrorism would facilitate the allocation of resilience and national security resources.

References

Abbas, M., Khan, F., Liou, Y. A., Ullah, H., Javed, B., & Ali, S. (2024). Assessment of the impacts of climate change on the construction of homogeneous climatic regions and ensemble climate projections using CMIP6 data over Pakistan. *Atmospheric Research, 304*, 107359. https://doi.org/10.1016/j.atmosres.2024.107359

Abbasi, K. R., Hussain, K., Haddad, A. M., Salman, A., & Ozturk, I. (2022). The role of financial development and technological innovation towards sustainable development in Pakistan: fresh insights from consumption and territory-based emissions. *Technological Forecasting and Social Change, 176*, 121444. https://doi.org/10.1016/j.techfore.2021.121444

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information, 15*(11), 682. https://doi.org/10.3390/info15110682

Adi, T. W., & Arijanti, S. (2025). Reputational risk in the social media era: A case study of crisis management strategies for major brands in Indonesia. *Oikonomia: Journal of Management Economics and Accounting, 2*(4), 38–48. https://doi.org/10.61942/oikonomia.v2i4.411

Adnan, M., Xiao, B., Bibi, S., Xiao, P., Zhao, P., & Wang, H. (2024). Addressing current climate issues in Pakistan: an opportunity for a sustainable future. *Environmental Challenges, 15*, 100887. https://doi.org/10.1016/j.envc.2024.100887

Ahmad, M., Asad, M., & Irtaza, A. (2023). Analysis of climate change policy of Pakistan; hurdles & loopholes. *Pakistan Review of Social Sciences (PRSS), 4*(2), 4–17. https://www.pakistanreview.com/index.php/PRSS/article/view/200

Ahmad, S., & Jahangir, J. (2023). Cyber Warfare: Emerging Non-Traditional Threat to Pakistan's Security. *Pakistan Horizon, 76*(2), 39–58. https://www.pakistan-horizon.piia.org.pk/index.php/pakistan-horizon/article/view/287

Ahmed, M., Abid, M., Malik, N. A., Ali, S., Zahid, A., Malik, A., & Cheema, M. (2025). Climate-Resilient Strategies for Sustainable Management of Water Resources and Agriculture. In *Climate Resilient and Sustainable Agriculture: Volume 2: Social and Transformative Strategies* (pp. 1–25). Cham: Springer Nature Switzerland.

Ahmed, Z. S., & Shahzad, R. (2021). The role of peace education in countering violent extremism in Pakistan: An assessment of non-governmental efforts. *Conflict, Security & Development, 21*(3), 199–222. https://doi.org/10.1080/14678802.2021.1943150

Akram, M. S., & Malik, R. (2023). Digital Shadows: The Menace of Cyber Espionage and Pakistan's National Security. *Journal of Development and Social Sciences, 4*(3), 855–864. https://doi.org/10.47205/jdss.2023(4-III)80

Akram, M. S., Mir, M. J., & Rehman, A. (2023). Dimension of cyber-warfare in Pakistan's context. *Journal of Positive School Psychology, 7*(6), 82–94. https://journalppw.com/index.php/jpsp/article/view/16941

Akram, M., & Safdar, M. R. (2025). Pakistan's content moderation paradox: combating violent radicalism in a competitive authoritarian regime. *Journal of Information Technology & Politics*. https://doi.org/10.1080/19331681.2025.2607035

Akram, N., & Tariq, K. (2024). War on Terrorism in Pakistan: Security Challenges and Safety Prioritization. *Social Science and Humanities Journal (SSHJ), 8*(04), 34765–34782. https://doi.org/10.18535/sshj.v8i04.981

Ali, A., Shah, M., Foster, M., & Alraja, M. N. (2025). Cybercrime Resilience in the Era of Advanced Technologies: Evidence from the Financial Sector of a Developing Country. *Computers, 14*(2), 38. https://doi.org/10.3390/computers14020038

Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: a comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry, 15*(12), 2175. https://doi.org/10.3390/sym15122175

Al-Saadi, A. S. A., & Khudari, M. (2024). The dynamic relationship between good governance, fiscal policy, and sustainable economic growth in Oman. *Journal of Infrastructure, Policy and Development, 8*(5), 3557. https://systems.enpress-publisher.com/index.php/jipd/article/view/3557

Anjum, U. (2020). Cyber crime in Pakistan; detection and punishment mechanism. *Časopis o društvenomitehnološkomrazvoju, 2*(2), 919062

Argyroudis, S. A., Mitoulis, S. A., Chatzi, E., Baker, J. W., Brilakis, I., Gkoumas, K., ... & Linkov, I. (2022). Digital technologies can enhance climate resilience of critical infrastructure. *Climate Risk Management, 35*, 100387. https://doi.org/10.1016/j.crm.2021.100387

Ashraf, S., Mustafa, G., & Ali, G. (2023). Pakistan's National Security Policy: An Analysis. *Annals of Human and Social Sciences, 4*(3), 177–176. http://doi.org/10.35484/ahss.2023(4-III)16

Babur, A., & Noor, S. (2023). Paigham-E-Pakistan AsA Counter Extremism Narrative. *Journal of Contemporary Studies, 12*(1), 69–87. https://jcs.ndu.edu.pk/index.php/site/article/view/246

Baloch, S. M. (2025). Accelerated glacial melt and monsoon rains trigger deadly floods in Pakistan. *The Guardian.* Online available at: https://www.theguardian.com/world/2025/jul/09/accelerated-glacial-melt-and-monsoon-rains-trigger-deadly-floods-in-pakistan (accessed on 25th January, 2026).

Belmin, R., Paulin, M., & Malézieux, E. (2023). Adapting agriculture to climate change: which pathways behind policy initiatives?. *Agronomy for Sustainable Development, 43*(5), 59. https://doi.org/10.1007/s13593-023-00910-y

Bilal, H., Khan, A., & Azhar, M. (2022). War on Terrorism and its Impacts on Pakistan's Security. *South Asian Studies, 36*(2)., 287–302. https://sasj.pu.edu.pk/9/article/view/1262

Bokhari, S. A. A. (2023). A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. *Social Sciences, 12*(11), 629. https://doi.org/10.3390/socsci12110629

Budiana, M., Muhammad , M. F., Djuyandi, Y. D., & Pancasilawan, R. P. (2023). Indonesia military power under the increasing threat of conflict in the South China Sea. *Central European Journal of International and Security CEJISS., 13*(4), 259–274.

Bugti, I. A. (2025). Climate Change and Water Crisis in Balochistan: Causes, Effects, and Pathways to Resilience. *Review Journal of Social Psychology & Social Works, 3*(2), 1269–1286. https://socialworksreview.com/index.php/Journal/article/view/281

Chaudhry, K. T. (2022). Environmental Policy Analysis of Pakistan: A Theoretical Perspective. *Journal of Development and Social Sciences, 3*(4), 507–521. https://doi.org/10.47205/jdss.2022(3-IV)48

Chou, M. H., Huisman, J., & Lorenzo, M. P. (2024). Regional cooperation in higher education. In *Handbook of Regional Cooperation and Integration* (pp. 266–288). Edward Elgar Publishing.

Dekker, M., & Alevizos, L. (2024). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy, 7*(1), e333. https://doi.org/10.1002/spy2.333

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences, 11*(10), 4580. https://doi.org/10.3390/app11104580

Elkhidir, E., Mannakkara, S., Henning, T. F., & Wilkinson, S. (2023). A pathway towards resilient cities: National resilience knowledge networks. *Cities, 136*, 104243. https://doi.org/10.1016/j.cities.2023.104243

FAO. (2023). *Pakistan: Floods response update, February 2023*. Rome. https://doi.org/10.4060/cc4663en

Fu, Q., & Zhang, X. (2024). Promoting community resilience through disaster education: Review of community-based interventions with a focus on teacher resilience and well-being. *PLoS ONE, 19*(1), e0296393. https://doi.org/10.1371/journal.pone.0296393

Fuentes, E. (2023). School Disaster Preparedness, Response and Recovery: Teachers in Focus. *Psychology and Education: A Multidisciplinary Journal, 12*(7), 646–668. https://ejournals.ph/article.php?id=21781

Ghalib, S. J. (2025). Reevaluating Conventional Strategies: Harnessing Traditional Structures to Counter Violent Extremism in Pakistan. *NUST Journal of International Peace & Stability, 8*(1), 62–76. https://doi.org/10.37540/njips.v8i1.186

Gillani, A. (2023). Determinants Of Indo-Pak Wars: Analysing Through Prism Of Waltz Three Images Of War. *Journal of Positive School Psychology, 7*(6), 447–457. https://journalppw.com/index.php/jpsp/article/view/17025

Hafeez, M. M., Ahmed, R. N., Khan, M. D., & Safdar, M. A. (2020). What are the Crisis and Issues of Governance in Pakistan? An Analysis. *Review of Applied Management and Social Sciences, 3*(1), 53–59. https://doi.org/10.47067/ramss.v3i1.24

Haq, I. U., & Zarkoon, S. M. (2023). Cyber Stalking: A Critical Analysis of Prevention of Electronic Crimes Act-2016 and Its Effectiveness in Combating Cyber Crimes, A Perspective from Pakistan. *Pakistan's Multidisciplinary Journal for Arts & Science, 4*(3), 43–62. https://doi.org/10.5281/zenodo.10450177

Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: an analysis of the cyber threat landscape and readiness. *IEEE Access, 11*, 40049–40063. https://doi.org/10.1109/ACCESS.2023.3268529

Hussain, B. (2025). Cybercrime surges 35% in Pakistan in 2025 amid govt's push for cryptocurrency legalization. *Business Recorder*, online available at: https://www.brecorder.com/news/40388687/cybercrime-surges-35-in-pakistan-in-2025-amid-govts-push-for-cryptocurrency-legalisation (accessed on 25th January, 2026).

Hussain, M., Butt, A. R., Uzma, F., Ahmed, R., Irshad, S., Rehman, A., & Yousaf, B. (2020). A comprehensive review of climate change impacts, adaptation, and mitigation on environmental and natural calamities in Pakistan. *Environmental Monitoring and Assessment, 192*, 1–20. https://doi.org/10.1007/s10661-019-7956-4

Hussain, N., & Bhatti, S. H. (2024). The Tightrope of Individual Liberties amid Pakistan's Counter-Terrorism Agenda. *Annals of Social Sciences and Perspective, 5*(1), 145–155. https://doi.org/10.52700/assap.v5i1.360

Imran, M., Murtiza, G., Akbar, M. S., Advocate, T. B., Azam, A., & Asif, M. (2024). Towards Environmental Justice: Evaluating Environmental Law in Pakistan. *Kurdish Studies, 12*(1), 5111–5124. https://doi.org/10.53555/ks.v12i1.3330

IPCC. (2022). *Climate Change 2022: Impacts, Adaptation, and Vulnerability* [Working Group II Contribution to the IPCC Sixth Assessment Report]. Cambridge University Press. Intergovernmental Panel on Climate Change, online available at; https://www.ipcc.ch/report/ar6/wg2/ (accessed on 25th January, 2026).

Irfan, A. (2022). Counter-Terrorism Strategy of Pakistan: A Case Study of Military Operations. Journal of Development and Social Sciences, 3(III), 843–855. https://doi.org/10.47205/jdss.2022(3-iii)79

Janjua, S., Hassan, I., Muhammad, S., Ahmed, S., & Ahmed, A. (2021). Water management in Pakistan's Indus Basin: challenges and opportunities. Water Policy, 23(6), 1329–1343. https://doi.org/10.2166/wp.2021.

Javaid, U. (2022). Accomplishments and Challenges of Pakistan's Fight against Violent Religious Extremism: A Critical Analysis. Pakistan Social Sciences Review, 6(II), 705–720. https://doi.org/10.35484/pssr.2022(6-ii)59

Kashif, M., Shah, S. Z. A., & Ahmad, M. (2025). Impact of Transnational Criminal Organizations on Political, Economic and Social Perspectives of Pakistan. Bulletin of Business and Economics (BBE), 14(1), 30–38. https://doi.org/10.61506/01.00575

Khan, B. A. (2025). Environmental Challenges and Geopolitical Tensions in South Asia: Migration, Conflict, and Cooperation. In: Nandy, D., Das, M. (eds) *Decoding the Chessboard of Asian Geopolitics*. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-96-3368-5_7

Khan, H. U., Khan, R. A., Alwageed, H. S., Almagrabi, A. O., Ayouni, S., & Maddeh, M. (2025). AI-driven cybersecurity framework for software development based on the ANN-ISM paradigm. Scientific Reports, 15(1), 13423. https://doi.org/10.1038/s41598-025-97204-y

Khan, M. A., & Naazer, M. A. (2023). Explaining the Role of Domestic Factors in Shaping Foreign Policies: India and Pakistan in Comparative Perspective (2014-2020). Journal of South Asian Studies, 11(2), 119–129. https://doi.org/10.33687/jsas.011.02.4818

Khan, M. B., Jaffar, S., Sajid, S., Atta, A., Ahmed, W., & Mukhtar, M. W. (2024). Alone Atomic Islamic State Pakistan's Significant Geo-Political Location For Super Powers Monopole Strategies Cultivation. *Kurdish Studies, 12*(4), 1537–1541. https://doi.org/10.53555/ks.v12i4.3215

Khan, M. K., & Wei, L. (2016). When friends turned into enemies: The role of the national state vs. Tehrik-i-Taliban Pakistan (TTP) in the war against terrorism in Pakistan.

Korean Journal of Defense Analysis, 28(4), 597–626. https://doi.org/10.22883/kjda.2016.28.4.007

Khattak, T., & Asghar, D. R. J. (2024). Strategic Counter Measures to Terrorism and Extremism in Pakistan and Insights from Home Land Security. Inverge Journal of Social Sciences, 3(1), 61–74. https://doi.org/10.63544/ijss.v3i1.76

Kidwai, S. A. (2022). Rivalry Between the Taliban and ISKP: The Collision of Terror. India Quarterly, 78(4), 544–557. https://doi.org/10.1177/09749284221127791

Kioskli, K., Grigoriou, E., Islam, S., Yiorkas, A. M., Christofi, L., & Mouratidis, H. (2025). A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain. International Journal of Information Security, 24(2), 1–28. https://doi.org/10.1007/s10207-025-01009-z

Kniep, R., Ewert, L., Reyes, B. L., Tréguer, F., Cluskey, E. M., & Aradau, C. (2023). Towards democratic intelligence oversight: Limits, practices, struggles. Review of International Studies, 14(1), 209–229. https://doi.org/10.1017/S0260210523000013

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. https://doi.org/10.1177/23477970211017719

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. In: Lehto, M., Neittaanmäki, P. (eds) *Cyber Security*. Computational Methods in Applied Sciences, vol 56. Springer, Cham. https://doi.org/10.1007/978-3-030-91293-2_1

Lopes, L. C. (2024). Climate Change as a Security Risk: Disruptive Impacts on the European Union's Defence-Related Critical Energy Infrastructure. *Nação e Defesa, 169*, 9–26. https://doi.org/10.47906/ND2024.169.01

Mahmood, K. (2022). Countering Violent Extremism through Narrative Building in Pakistan. Islamic Studies, 61(1), 63–84. https://doi.org/10.52541/isiri.v61i1.2273

Makki, M., Butt, F. A., Akash, S. A., Petrova, K., & Naeem, S. A. (2025). Fragile Geographies and the Climate-Conflict Nexus: Investigating Climate-Induced Security Risks, Migration, and Inequality in Balochistan, Pakistan. Alternatives, 50(2), 350–375. https://doi.org/10.1177/03043754241291728

Mashwama, N. X., & Phesa, M. (2025). Systematic Review of Multidimensional Assessment of Coastal Infrastructure Resilience to Climate-Induced Flooding: Integrating Structural Vulnerability, System Capacity, and Organizational Preparedness. Climate, 13(9), 192. https://doi.org/10.3390/cli13090192

Medellín-Azuara, J., Escriva-Bou, A., Gaudin, A. C., Schwabe, K. A., & Sumner, D. A. (2024). Cultivating climate resilience in California agriculture: Adaptations to an increasingly volatile water future. *Proceedings of the National Academy of Sciences, 121*(32), e2310079121. https://doi.org/10.1073/pnas.2310079121

Mehboob, M. S., & Kim, Y. (2021). Effect of climate and socioeconomic changes on future surface water availability from mountainous water sources in Pakistan's

Upper Indus Basin. Science of the Total Environment, 769, 144820. https://doi.org/10.1016/j.scitotenv.2020.144820

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. International Journal of Research in Business and Social Science (2147- 4478), 11(4), 384–396. https://doi.org/10.20525/ijrbs.v11i4.1714

Mumtaz, M. (2018). The National Climate Change Policy of Pakistan: An evaluation of its impact on institutional change. *Earth Systems and Environment, 2*(3), 525–535. https://doi.org/10.1007/s41748-018-0062-x

Mustafa, G., Murtaza, Z., & Murtaza, K. (2020). Cyber Warfare between Pakistan and India: Implications for the Region. *Pakistan Languages and Humanities Review, 4*(1), 59–71. https://doi.org/10.47205/plhr.2020(4-I)2.05

Muzamil, M. R., Boruff, B., Shahbaz, B., Khan, N. A., Sattar, R. S., & Hafeez, M. (2024). Climate futures and development pathways: A journey from terrorism to tourism in the Khyber-Pakhtunkhwa Province of Pakistan. *Futures, 158*, 103344. https://doi.org/10.1016/j.futures.2024.103344

NCSP. (2021). *National Cyber Security Policy 2021*. Ministry of Information Technology & Telecommunication, Government of Pakistan. Online available at: https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf (accessed on 25th January, 2026).

NDMA. (2025). *Post Monsoon Review 2025*. National Disaster Management Authority (Pakistan), National Institute of Disaster Management. https://www.ndma.gov.pk/storage/publications/December2025/NUgyCMG8uMfYsFhVMXka.pdf (accessed on 25th January, 2025).

Nie, Y., Pritchard, H. D., Liu, Q., Hennig, T., Wang, W., Wang, X., & Chen, X. (2021). Glacial change and hydrological implications in the Himalaya and Karakoram. *Nature Reviews Earth & Environment, 2*(2), 91–106. https://doi.org/10.1038/s43017-020-00124-w

Noor, H., Seelro, D. K., & Ali, S. A. (2024, January). Review of National Cybersecurity Policies: A Case Study on Asian Countries. In *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)* (pp. 1–6). IEEE.

NR3C. (2023). National Response Centre for Cyber Crime (NR3C) – Pakistan. Online available at: https://www.cybersecurityintelligence.com/national-response-centre-for-cyber-crime-nr3c-pakistan-2086.html (accessed on 25th January, 2026).

Nyman, J. (2023). Securitization. In *Security Studies* (pp. 115–130). Routledge.

Ong'esa, I. G., & Muoka, B. (2025). Counter-terrorism Strategies in Mombasa County: Analyzing Implementation Approaches to Mitigate Radicalization. *Journal of African Interdisciplinary Studies, 9*(3), 120–130. https://ir-library.ku.ac.ke/handle/123456789/31537

Park, J. (2026). India and Pakistan in Central Asia: Competition and Cooperation. In *Emerging Partners of Central Asia: Engagement of Small and Middle Powers* (pp. 241–259). Cham: Springer Nature Switzerland.

Pashentsev, E. N., & Kolotaev, Y. Y. (2025). Information and communication technologies in political crisis management: resilience, forecasting, and response. *Discover Global Society, 3*(1), 84. https://doi.org/10.1007/s44282-025-00216-2

PDNA. (2022). *Pakistan Floods 2022: Post-Disaster Needs Assessment*. Online available at: https://thedocs.worldbank.org/en/doc/4a0114eb7d1cecbbbf2f65c5ce0789db-0310012022/original/Pakistan-Floods-2022-PDNA-Main-Report.pdf (accessed on 25th January, 2026).

PECA. (2016). *Prevention of Electronic Crimes Act, 2016*. Online available at: https://www.na.gov.pk/uploads/documents/1470910659_707.pdf (accessed on 25th January, 2026).

Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology, 9*(1), 28–78. https://doi.org/10.1080/23742917.2024.2312671

Rahman, H., Sadiq, A., & Shah, S. A. (2023). Resurgence and Response: Evaluating the Effectiveness of Pakistan's Counter-Terrorism Strategies amidst Rising Terrorism Threats. *Pakistan Journal of Social Research, 5*(04), 24–37. https://doi.org/10.52567/pjsr.v5i04.1329

Rashid, M. T., Fatima, R., & Wasif, M. (2023). War on Terror: The Cost Pakistan Paid. *Annals of Human and Social Sciences, 4*(2), 738–750. https://doi.org/10.35484/ahss.2023(4-II)67

Rehman, M. Z. U., Ishaque, W., & Sayed, M. H. A. K. (2025). Emerging dynamics and national security of Pakistan: Challenges and strategies. *Research Consortium Archive, 3*(1), https://doi.org/228–240. 10.62019/qxm59t12

Reiter, K., Knittel, N., Bachner, G., & Hochrainer-Stigler, S. (2022). Barriers and ways forward to climate risk management against indirect effects of natural disasters: A case study on flood risk in Austria. *Climate Risk Management, 36*, 100431. https://doi.org/10.1016/j.crm.2022.100431

Rose, A. Z. (2009). A framework for analyzing the total economic impacts of terrorist attacks and natural disasters. *Journal of Homeland Security and Emergency Management, 6*(1). https://doi.org/10.2202/1547-7355.1399

Saad, S., Mahsud, M. I., & Mian, G. (2024). Climate change impacts: exploring the rising climate-security nexus in Pakistan. *Liberal Arts and Social Sciences International Journal (LASSIJ), 8*(1), 177–190. https://doi.org/10.47264/idea.lassij/8.1.10

SATP. (2025). Terrorism assessment: Pakistan 2025. *South Asia Terrorism Portal*, Online available at: https://www.satp.org/terrorism-assessment/pakistan (accessed on 25th January, 2026).

Shah, S., Shah, M. N. U. H., & Abbas, S. (2024). Pak-Iran Convergence and Divergence of Interests During 2005-2015. *Shnakhat, 3*(3), 142–153. https://doi.org/10.33687/jsas.010.02.4262

Shahzad, S. A., Anser, M. K., Haq, I. U., Aamir, A., & Zaman, K. (2026). Deploying artificial intelligence in warfare and national security: A qualitative exploration of strategic implications for Pakistan. *Global Change, Peace & Security*. https://doi.org/10.1080/14781158.2025.2611230

Siloko, B. E. (2024). Human security, sustainable livelihoods and development: the case of the Niger Delta region in Nigeria. *Global Discourse, 14*(2-3), 411–432. https://doi.org/10.1332/20437897Y2024D000000037

Song, Y., Zhang, Z., Sahut, J. M., & Rubin, O. (2023). Incentivizing green technology innovation to confront sustainable development. *Technovation, 126*, 102788. https://doi.org/10.1016/j.technovation.2023.102788

Stoddart, K. (2022). Non and sub-state actors: Cybercrime, terrorism, and hackers. In *Cyberwarfare: threats to critical infrastructure* (pp. 351–399). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6

Sultan, N., Rehman, A. U., Khan, A. N., & Tanvir, R. (2024). Pakistan's Military Operations in Erstwhile Fata and De-Radicalization Process in Education Sector after 2014. *Pakistan JL Analysis & Wisdom, 3*, 194.

Syahputra, A. R., & Hamid, S. (2024). Contemporary Perspective on Terrorism: A Literature Review. *JMKSP (Jurnal Manajemen, Kepemimpinan, dan Supervisi Pendidikan), 9*(1), 347–366. https://doi.org/10.31851/jmksp.v9i1.14297

Tahir, M., Farrukh, T., & Shahid, M. (2019). Cyber Laws and Cyber Security in Pakistan: Myths and Realities. *Global Social Sciences Review (GSSR), 4*(1), 485–493.

Tula, O. A., Daraojimba, C., Eyo-Udo, N. L., Egbokhaebho, B. A., Ofonagoro, K. A., Ogunjobi, O. A., ... & Banso, A. A. (2023). Analyzing global evolution of materials research funding and its influence on innovation landscape: a case study of us investment strategies. *Engineering Science & Technology Journal, 4*(3), 120–139. https://doi.org/10.51594/estj.v4i3.556

Ullah, S., Xiaopeng, D., Anbar, D. R., Amaechi, C. V., & Ashraf, M. W. (2025). Political risk management in international construction: Evidence from Pakistan. *Global Journal of Flexible Systems Management, 26*, 839–864. https://doi.org/10.1007/s40171-025-00463-x

Usman, M., Ali, A., Baig, S. A., Radulescu, M., Abbas, A., & Akram, R. (2025). Food security in Punjab, Pakistan: rural views on climate disasters and their impacts. *Environment, Development and Sustainability*. https://doi.org/10.1007/s10668-025-06047-0

Vajravelu, A., Ashok Kumar, N., Sarkar, S., & Degadwala, S. (2023). Security Threats of Unmanned Aerial Vehicles. In: Jahankhani, H., El Hajjar, A. (eds) *Wireless Networks*. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-33631-7_5

Verma, R. (2020). China's new security concept: India, terrorism, China's geostrategic interests and domestic stability in Pakistan. *The Pacific Review, 33*(6), 991–1021. https://doi.org/10.1080/09512748.2019.1663902

Wahab, F. (2024). The consequences of Pakistan's counterterrorism policies: socio-cultural and political transformation in tribal districts. *Critical Studies on Terrorism, 17*(3), 581–605. https://doi.org/10.1080/17539153.2024.2360271

Wang, N., Wu, M., & Yuen, K. F. (2023). Assessment of port resilience using Bayesian network: A study of strategies to enhance readiness and response capacities. *Reliability Engineering & System Safety, 237*, 109394. https://doi.org/10.1016/j.ress.2023.109394

Yongmei, C., & Afzal, J. (2023). Impact of enactment of 'the prevention of electronic crimes act, 2016' as legal support in Pakistan. *Academy of Education and Social Sciences Review, 3*(2), 203–212. https://doi.org/10.48112/aessr.v3i2.500

Yousaf, A., Kiran, A., Iqbal, M. A., Murtiza, G., & Hussain, M. (2025). Climate change effects on rural livelihoods in Pakistan: legal and policy analysis. *GeoJournal, 90*(1), 25. https://doi.org/10.1007/s10708-024-11273-6