THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

CYBER SECURITY THREATS AND ELECTRONIC CRIMES: A CRITICAL ANALYSIS OF 5TH GENERATION WARFARE IN PAKISTAN

Muhammad Mehroosh Sheikh
Graduated from Bahria University Law School, Bahria University Islamabad Campus (BUIC)
mehrooshsheikh95@gmail.com
Sumera Shahmir
Graduated from Bahria University Law School, Bahria University Islamabad Campus (BUIC)
sumerashahmir29@gmail.com
Dr. Sohaib Mukhtar
Associate Professor, HOD (Research), NUST Law School, National University of Sciences & Technology (NUST)
sohaibmukhtar@nls.nust.edu.pk

Abstract

This research critically examines legal and strategic implications of 5th Generation Warfare (5GW) in Pakistan, with a specific focus on cyber threats and electronic crimes. Through an in-depth analysis of Pakistan's domestic legal framework, including the Prevention of Electronic Crimes Act (PECA) 2016 alongside proposed data protection laws. This study identifies significant legislative and enforcement gaps that hinder effective cyber defense. Comparative evaluations of India, Israel, United States, China, and Germany reveal how other states have fortified their legal and strategic readiness against hybrid threats. Furthermore, this research analyzes case studies involving cyber-attacks, disinformation campaigns, and psychological operations to highlight Pakistan's vulnerabilities. International instruments such as Tallinn Manual, UN GGE norms, and Budapest Convention are also explored to emphasize the importance of integrating global cyber norms into Pakistan's national policy. This research concludes by proposing comprehensive reforms, including the establishment of unified National Command for Cyber and Hybrid Warfare, bridging civil-military gaps, and fostering societal resilience against 5GW tactics. Ultimately, this study underscores the urgent need for Pakistan to recognize 5GW as a strategic national security threat and implement robust legal and institutional defenses to safeguard its sovereignty and ideological unity.

Keywords: *Fifth-Generation Warfare (5GW); Cyber Threats of Electronic Crimes; PECA 2016; Pakistan National Security; Cyber Law; Psychological Warfare; Hybrid Threats.*

Introduction

The evolution of warfare into the fifth generation (5GW) has introduced new threats to national security, manifesting through cyber-attacks, disinformation campaigns, and psychological operations. Pakistan is a frontline state, faces severe vulnerabilities due to its fragmented legal frameworks and underdeveloped cyber defense mechanisms. While legislative efforts like PECA 2016 and the Data Protection Bill attempt to regulate the digital domain, gaps in enforcement, jurisdiction, and institutional preparedness persist. This research critically examines Pakistan exposure to 5GW tactics, assesses the efficacy of its legal instruments, and proposes comprehensive legal and strategic reforms to safeguard national sovereignty and societal unity.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

In the contemporary era, warfare evolved beyond traditional battlefields and conventional combat, entering a new domain characterized by ambiguity, deception, cyber operations, and psychological manipulation. This paradigm shift is termed Fifth-Generation Warfare (5GW), a mode of conflict where the primary weapons are not guns and tanks, but information, perception, and cyberspace. 5GW strategies aim to destabilize states internally by targeting ideological foundations, undermining public trust, manipulating narratives, and exploiting social, ethnic, and political fault lines without engaging in open hostilities.

Pakistan, due to its geopolitical position and internal vulnerabilities, has become a prominent target of 5GW tactics. The rise of cyber threats, disinformation campaigns, hybrid attacks on critical infrastructure, and the psychological exploitation of ethnic and regional divides underscore the urgency for a comprehensive strategic and legal response. Although Pakistan has taken important steps to legislate in the cyber domain, notably through the Prevention of Electronic Crimes Act (PECA) 2016 and the Data Protection Bill remain largely reactive, fragmented, and insufficiently aligned with the complex realities of 5GW.

Given the increasing scale of hybrid threats, Pakistan's national security apparatus must evolve to recognize 5GW as an existential challenge requiring multidimensional reforms. This research critically analyzes the manifestation of 5GW in Pakistan, examines the gaps in existing cyber laws, strategic policies and proposes a way forward by drawing insights from international legal instruments and successful global models. Addressing these challenges is vital for protecting Pakistan sovereignty, ideological unity, and future stability.

This study adopts doctrinal research methodology to critically analyze the legal and strategic implications of Fifth-Generation Warfare (5GW) in Pakistan, particularly focusing on cyber threats and electronic crimes. A multi-pronged approach has been utilized, combining literature review, legal analysis, case study examination, comparative study, and documentary and judicial analysis to ensure a comprehensive and critical exploration of the topic.

A detailed legal analysis has been conducted of Pakistan primary legal instruments dealing with electronic crimes and cyber threats, namely the Prevention of Electronic Crimes Act (PECA) 2016, the Electronic Transactions Ordinance (ETO) 2002, and the Personal Data Protection Bills of 2018 and 2023. These statutes are critically evaluated to determine their strengths and limitations in countering hybrid and cyber warfare challenges linked to 5GW. Special attention is given to the 2025 amendments to PECA and the emerging institutional mechanisms like the Social Media Protection and Regulatory Authority (SMPRA) and the National Cyber Crime Investigation Agency (NCCIA). A comparative analysis is employed to examine the cyber defense frameworks, legislative responses, and strategic countermeasures of selected countries such as India, Israel, the United States, Germany, and China. These comparative insights help in identifying best practices and strategic models that can be adapted to Pakistan legal and national security framework to enhance resilience against 5GW threats.

Understanding Fifth-Generation Warfare

Traditionally, war has been perceived through the lens of physical confrontation marked by weapons, soldiers, and defined battlefields. However, as the nature of global conflict has evolved over successive generations, the current phase, known as Fifth-Generation Warfare (5GW),

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

departs radically from these conventions. In 5GW, the battlefield is no longer physical but cognitive, informational, and digital. It operates through non-kinetic tools such as disinformation, cyber intrusion, and psychological manipulation tools that target perceptions rather than physical assets. This evolution signals not merely a shift in strategy, but a redefinition of what constitutes warfare in the modern age. The lines between war and peace, combatants and civilian, have become increasingly blurred, requiring a renewed understanding of conflict in the 21st century. In the 21st century, the concept of warfare has evolved far beyond conventional definitions. Traditional conflict marked by direct combat, physical battlegrounds, and visible enemy forces are now being overshadowed by a more covert and complex form of warfare known as Fifth-Generation Warfare (5GW). Unlike its predecessors from First to Fourth Generation Warfare, which relied on conventional battles and kinetic force, 5GW is defined by psychological influence, digital tools, and information manipulation to subvert the enemy without direct confrontation. Fifth-Generation Warfare is fundamentally non-kinetic, meaning it does not rely on traditional weapons or force. Instead, it operates through the manipulation of information, the execution of cyber-attacks, the dissemination of disinformation, and the exploitation of public perception. It targets a nation's political, economic, and social stability by shaping narratives, creating confusion, and fostering distrust. In this type of warfare, the objective is not necessarily to conquer territory, but to weaken a state from within by disrupting its institutions, polarizing its society, and undermining public confidence in leadership, systems, and truth itself.[1]

The emergence of 5GW as a recognized paradigm occurred in the late 2000. The term was notably discussed by David Axe in a 2009 article in Wired magazine and later expanded upon in scholarly and military discourse. Analysts began identifying a shift in conflict one no longer defined by conventional force but by the strategic use of information and perception. Authors such as Daniel Abbott, in his Handbook of 5GW, emphasized that the very nature of this generation of warfare is its difficulty to define. Military historian Martin van Creveld further noted that 5GW blurs the lines between war and peace, creating prolonged ambiguity and strategic uncertainty. This recognition marked a turning point in security studies, prompting military and policy institutions to reconsider the boundaries of modern warfare and the role of non-military tools in national power. What distinguishes 5GW from previous generations of warfare is its ambiguity and invisibility. It is often waged in what scholars refer to as the "grey zone" a space between peace and open conflict, where hostile actions are deliberate yet difficult to attribute. A cyber-attack, for example, may originate from an untraceable location; a propaganda campaign may be driven by anonymous accounts on social media; and a state actor may direct psychological operations through third parties while denying all responsibility. This level of deniability is a central feature of 5GW, making it challenging for targeted states to respond through conventional military or legal means.[2]

The emergence of 5GW is not theoretical, it has already manifested through real-world incidents that have reshaped global perceptions of conflict. One prominent example is Russia's interference

[1] Krishnan, A. (2022). Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict. *Journal of Strategic Security*, *15*(4), 14-31.

[2] Krishnan, A. (2024). *Fifth Generation Warfare: Dominating the Human Domain*. Routledge.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

in the 2016 United States presidential election. Through the strategic use of social media platforms, Russian operatives disseminated disinformation, amplified divisive political narratives, and manipulated public discourse with the intention of eroding democratic trust rather than achieving territorial gain. Similarly, the Stuxnet cyber-attack widely attributed to the United States and Israel successfully sabotaged Iran nuclear centrifuges by deploying malicious code that disrupted physical infrastructure without any physical confrontation. The 2021 Colonial Pipeline ransom ware attack in the U.S, demonstrated how a faceless cyber operation could paralyze a critical national asset, trigger public panic, and lead to major economic consequences all without the involvement of military troops or traditional combat. These examples illustrate that in Fifth-Generation Warfare, the battlefield is no longer confined to geographic space. It extends into cyberspace, financial systems, media networks, and even the minds of individuals. What makes this form of warfare even more concerning is the accessibility of its tools. Unlike traditional war, which required armies, weapons, and state infrastructure, 5GW enables non-state actors, small organizations, and even individuals to launch attacks using relatively low-cost resources such as social media, malware, and psychological messaging. This has led to the democratization of conflict, where influence and disruption are no longer the sole domain of powerful nations.[3]

At its core, Fifth-Generation Warfare is a battle for influence and perception. It aims to control the narrative, shape public opinion, and destabilize a society from within all while avoiding direct confrontation. As such, it poses an unprecedented challenge to national and global security. Understanding the nature and scope of 5GW is therefore not just essential, it is foundational for any serious legal or strategic response in today digital age. Fifth-Generation Warfare (5GW) encompasses a broad array of non-traditional, non-kinetic tactics that operate beyond the boundaries of conventional military engagement. Unlike earlier generations of warfare, which were fought with physical weapons and uniformed armies, 5GW is waged invisibly through narratives, digital networks, information systems, and psychological influence. It aims to undermine a state internal stability without the need for formal declaration of war.[4]

The arsenal of 5GW is extensive. It includes cyber-attacks, disinformation, psychological operations, economic coercion, legal manipulation, media distortion, covert influence campaigns, and surveillance-based control mechanisms. These tools are often used in combination to create confusion, fear, and societal disruption. Among these, cyber warfare, disinformation, and psychological manipulation represent the most significant dimensions of 5GW, particularly in the context of cyber threats and electronic crimes. Cyber warfare stands at the forefront of 5GW tactics. It involves the calculated use of digital technologies to infiltrate, disrupt, or damage an adversary technological infrastructure. These attacks frequently target critical sectors such as energy, finance, healthcare, and communications, often resulting in operational paralysis. A widely studied example is the Stuxnet operation, which disabled Iran nuclear centrifuges through a stealth

[3] Kelshall, C. M. (2022). Fifth Generation Warfare? Violent Transnational Social Movements as Security Disruptors. in *Disruption, Ideation and Innovation for Defence and Security* (pp. 269-298). Cham: Springer International Publishing.

[4] Adamson, A., & Snyder, M. (2017). The Challenges of Fifth-Generation Transformation. *The Rusi Journal*, *162*(4), 60-66.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

malware attack achieving strategic objectives without kinetic force.[5]

Similarly, the Colonial Pipeline ransom ware attack in 2021 disrupted fuel distribution across the United States, causing public panic and economic uncertainty. The Greenburg attack, identified in international cyber security reports, further illustrates the capability of cyber actors to compromise essential infrastructure. These examples highlight how cyberspace has become a principal domain of conflict, enabling adversaries to bypass conventional force through digital sabotage. Disinformation constitutes another core instrument of 5GW. It involves the deliberate dissemination of false, misleading, or manipulated information intended to distort public perception, provoke division, and delegitimize institutions. Within this framework, control over the information environment becomes more decisive than territorial control. A key illustration is the Russian interference in the 2016 United States presidential election, where coordinated digital campaigns exploited social media platforms to influence voter behavior, intensify polarization, and weaken democratic confidence. Disinformation strategies often exploit social media algorithms, inauthentic accounts, and emotionally charged content to amplify divisive narratives. The central threat lies not only in the spread of falsehoods, but in the erosion of shared reality, which is essential to national cohesion and democratic resilience.[6]

Psychological manipulation, also known as psychological warfare or PsyOps, targets the emotional and cognitive dimensions of individuals and populations. These tactics are designed to undermine morale, generate confusion, foster fear, and subtly alter behavior through sustained influence. Methods may include surveillance, targeted harassment, the deployment of spyware such as Pegasus, reportedly used to monitor journalists and political figures and the creation of digitally altered content, including deep fake videos. These operations are intended to instill distrust, promote self-censorship, and degrade public confidence in democratic processes. In the context of 5GW, psychological manipulation transforms the human mind into a critical battleground, where influencing thought becomes a strategic objective. The effectiveness of these tactics is further magnified by their accessibility and plausible deniability. With the rise of open-source technology, inexpensive malware, and global digital platforms, even non-state actors, lone individuals, or small ideological groups can conduct high-impact cyber operations. The anonymity inherent in digital environments allows these actors to deny involvement, avoid attribution, or redirect blame complicating legal recourse and diplomatic response. The defining characteristic of these tactics lies in their ability to fragment and destabilize societies from within. Through the exploitation of digital vulnerabilities, manipulation of narratives, and targeting of human psychology, 5GW presents challenges that traditional security mechanisms are ill-equipped to address. The strategic and legal dimensions of this evolving threat demand urgent attention, particularly in states where institutional frameworks and cyber security capacities remain in the process of development.[7]

[5] Qureshi, W. A. (2019). Fourth-and Fifth-Generation Warfare: Technology and Perceptions. *San Diego International Law Journal*, *21*, 187.

[6] Patel, A. (2019). Fifth-Generation Warfare and the Definitions of Peace. *The Journal of Intelligence, Conflict, and Warfare*, *2*(2), 15-28.

[7] Khan, A. M. (2025). 5th Generation Warfare and the Erosion of Traditional State Power: Analyzing Non-Kinetic Strategies in Modern Conflict. *International Journal of Social Sciences Bulletin*, *3*(3), 915-924.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Fifth-Generation Warfare Manifestation in Pakistan

Historically, Pakistan's security concerns have revolved around conventional military threats, particularly territorial disputes with India. However, the nature of warfare has evolved. From kinetic operations to ideological subversion, Pakistan now finds itself during Fifth-Generation Warfare (5GW) a form of conflict that exploits information, perception, and psychological operations to destabilize nations from within. The first official recognition of this transformation came in 2016, when General Raheel Sharif, then Chief of Army Staff (COAS), warned of "sub-conventional threats" and highlighted the emerging domain of invisible warfare targeting Pakistan internal coherence. In the same year, Major General Asif Ghafoor, serving as Director General of Inter-Services Public Relations (DG ISPR), popularized the term "5th Generation War" on digital platforms. He praised the voluntary efforts of Pakistan digital defenders and consistently portrayed media manipulation and digital warfare as new battlegrounds for national survival. In 2019, General Qamar Javed Bajwa, in his Defense Day address, warned that 5GW posed a real threat to Pakistan sovereignty, urging synchronization of civil and military policy responses. He described it as a hybrid challenge that included disinformation, psychological destabilization, and internal ideological attacks. His statements institutionalized the threat in the strategic lexicon of Pakistan security doctrine. This understanding was further deepened in 2021, when DG ISPR Major General Babar Iftikhar referred to India anti-Pakistan propaganda campaigns as a "major onslaught" of 5GW. In an interview with Global Village Space, he exposed how Pakistan economy, military, and international image were being strategically attacked through misinformation, particularly surrounding CPEC. He cited the false portrayal of Karachi building explosion as "civil war" by Indian media as a direct example.[8]

Prime Minister Imran Khan, addressing the 75th United Nation General Assembly in September 2020, highlighted the coordinated disinformation network targeting Pakistan image abroad. He condemned Indian efforts to create chaos in the region through fake news, digital propaganda, and ideological warfare firmly placing 5GW as a threat to Pakistan sovereignty and stability. Most recently, in 2023, COAS General Asim Munir emphasized the operational preparedness for conventional, sub-conventional, and 5GW, citing an exposed nexus between internal and external actors working to destabilize Pakistan. Prime Minister Shehbaz Sharif, in various addresses, echoed concerns about coordinated international efforts to economically and diplomatically isolate the country. These acknowledgments reflect Pakistan increasing vulnerability to non-kinetic operations. Cases like the 2020 cyber-attacks on K-Electric, the Pakistan Stock Exchange, and the National Bank of Pakistan demonstrate how foreign-sponsored malware and ransom ware attacks can cripple financial and utility systems. Furthermore, campaigns like APT29, documented in cyber security reports, show how digital surveillance and espionage now operate in the shadow of military conflict.[9]

However, the tactical reach of 5GW extends beyond infrastructure it targets human capital,

[8] Nadeem, Muhammad Ashraf, Ghulam Mustafa, and Allauddin Kakar. "Fifth Generation Warfare and its Challenges to Pakistan." *Pakistan Journal of International Affairs* 4, no. 1 (2021): 216-230.

[9] Jahangir, Javeria, and Naheed Bashir. "Fifth Generation Warfare: Response Strategy of Pakistan." *Academic Journal of Social Sciences (AJSS)* 6, no. 2 (2022): 59-76.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

particularly Pakistan youth. Economic inequality, educational constraints, and joblessness have created a frustrated demographic, vulnerable to digital radicalization. According to research, foreign-funded NGOs, online influencers, and ideological platforms exploit these frustrations to promote civil disobedience disguised as activism. Students and unemployed graduates are especially vulnerable to recruitment for digital protests, narrative disruption, and cyber warfare. This vulnerability is particularly acute in Baluchistan, where youth from impoverished and neglected communities are recruited and radicalized by separatist groups like Baluchistan Liberation Army (BLA). Under the guise of liberation, these groups are often backed by external actors and work to sow discontent through disinformation campaigns and social media propaganda. Their messaging appeals to themes of ethnic marginalization and injustice hallmarks of 5GW ideology. Several real-world cases highlight the psychological manipulation used in these campaigns. Najibullah, a former BLA member, revealed he was radicalized at the age of 14 with revolutionary literature and ideological indoctrination. Talat Aziz, a university student, was misled by Baloch student councils and promised a noble cause under separatist banners. Adila Baloch, a trained nurse, was deceived into preparing for a suicide attack in Turbat, manipulated through false promises of empowerment. These cases demonstrate the dangerous effectiveness of psychological manipulation by external actors. This psychological warfare has been facilitated by the porous border with Afghanistan the longest and historically least secured frontier of Pakistan. The absence of proper fencing and advanced surveillance along this border has made it easier for India and Afghanistan to influence youth in Khyber Pakhtunkhwa and Baluchistan, facilitating the flow of radical material, operatives, and anti-state narratives into tribal areas. Following the post-9/11 era, Pakistan involvement in the global War on Terror resulted in multiple military operations in the tribal areas of Khyber Pakhtunkhwa and Baluchistan, such as Operation Zarb-e-Azb. While these actions dismantled many terrorist networks, they also led to significant civilian displacement, infrastructure damage, and social fragmentation. Despite these sacrifices, the United States and European Union persistently demanded that Pakistan "do more", casting doubt on its counterterrorism commitments.[10]

Adding to this external pressure, India and Afghanistan launched coordinated psychological warfare, branding Pakistan a "terrorist haven" an accusation not rooted in facts but amplified through digital propaganda. A particularly damaging narrative emerged that Pakistan was fighting terrorism only for U.S. dollars. This idea was reinforced by the U.S. drone strikes in tribal areas, which caused immense civilian casualties. These strikes, while conducted without Pakistan full control, were used by hostile actors to suggest that Pakistani military was complicit in foreign attacks on its own citizens fueling resentment among already marginalized communities. Together, these conditions created a volatile narrative space where young people already disillusioned by socioeconomic inequality were easily swayed by anti-state propaganda. This manipulation formed a core pillar of hybrid warfare aimed at weakening national unity and institutional trust. This vacuum of trust and governance has been exploited by external adversaries through 5GW to

[10] Nawaz, Adnan, Muhammad Zeeshan, and Sufyan Akhlaq. "Fifth-Generation Warfare: A Quagmire and Fiasco to National Solidity of Pakistan." *South Asian Studies* 38, no. 01 (2023): 53-72.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

promote anti-state narratives, especially targeting the military. Neighboring states have strategically used media and digital platforms to amplify separatist sentiments and fuel comparisons to the 1971 situation, encouraging slogans of independence and rebellion in the affected regions.[11]

The Pashtun Tahafuz Movement (PTM), while initially grounded in legitimate grievances surrounding enforced disappearances and civilian casualties, quickly transformed into a platform for widespread anti-state messaging. The movement garnered considerable support from youth in Khyber Pakhtunkhwa and Baluchistan, particularly through its strong digital presence and emotionally resonant narratives. PTM leaders frequently used social media platforms like Twitter and Facebook to run campaigns portraying the military as an occupying force, employing hashtags such as #DollarArmy to suggest that Pakistan armed forces served foreign interests in exchange for financial aid. This framing sought to delegitimize counterterrorism operations by equating them with foreign interference and internal oppression. These sentiments were further amplified by PTM alleged coordination with Afghan-based sympathizers and media outlets, which served to externally reinforce the movement narrative inside Pakistan. This confluence of local grievances and cross-border media amplification created a potent form of fifth generation warfare through psychological manipulation and disinformation, systematically eroding trust in national institutions and showing disillusionment among an already vulnerable youth demographic.[12]

The arrest of Indian spy Kulbhushan Jadhav in 2016 further highlighted the coordinated and covert infiltration of Pakistani territory for the purpose of sabotage, psychological warfare, and disinformation. His presence and confession revealed how foreign intelligence agencies actively work to exploit local divisions and destabilize national institutions through both physical and narrative warfare. Alongside these campaigns, several international media outlets have increasingly highlighted allegations of election rigging in Pakistan, particularly in 2013, 2018 and 2024 general elections. Reports by platforms such as the Guardian and Voice of America (VOA) not only questioned the transparency of the electoral process but also resonated deeply with Pakistan's politically active youth. These narratives contributed to public disillusionment, protests, and a perceived breakdown of democratic legitimacy. As part of 5GW, such external amplification of political instability serves to fracture the citizen-state relationship, delegitimize governance structures, and undermine global standing of Pakistan.[13]

Pakistan's regional and sectarian tensions also serve as fertile ground for psychological manipulation. Disinformation campaigns promote the idea of structural oppression against ethnic minorities, often tied to groups like PTM. These narratives, frequently amplified by international media, turn local grievances into strategic tools for global pressure. In this broader context of hybrid aggression, India has increasingly deployed 5GW tactics to destabilize Pakistan using all elements of its national power. As per the Director General (DG) of Inter Services Personal

[11] Kamboh, Muhammad Khalique, Ghulam Mustafa, and Muhammad Fazal Rasul. "5th Generation Warfare and Issues of National Integration in Pakistan." *Pakistan Social Sciences Review* 5, no. 1 (2021): 802-814.

[12] Abawe, Zulfia. "A Relational Analysis of the Pashtun Tahafuz Movement (PTM) in Pakistan." *Ethnopolitics* (2026): 1-22.

[13] Mahmood, Sohail. "A Tumultuous Election Day in Pakistan: The 2024 General Election Turmoil." *International Policy Digest* (2024).

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Relations (ISPR), the Indian strategy targets Pakistan's information systems, economy, armed forces, and international image. The EU Disinfo Lab report exposed India's disinformation network involving ghost NGOs and fake media outlets aimed at influencing international bodies like the European Parliament and UNHRC. These tactics are designed to damage Pakistan's reputation and undermine its credibility on the world stage. Additionally, Indian attempts to sabotage the China-Pakistan Economic Corridor (CPEC) through terrorism and misinformation, along with its lobbying efforts that contributed to Pakistan's placement on the FATF grey list, exemplify the strategic use of hybrid warfare. While Pakistan has taken proactive military and diplomatic measures to counter these threats, the situation demands a calibrated national response that strengthens internal resilience, media capacity, counterintelligence, and information transparency.[14]

The ideological foundation of Pakistan is deeply rooted in the concept of Islamic unity and national integration. Quaid-e-Azam Muhammad Ali Jinnah envisioned a state where religious harmony would override ethnic, linguistic, and regional divisions. 5GW directly attacks this ideological core, aiming to fracture public loyalty to shared values and dismantle the narrative of unity. The primary goal of the fifth-generation operations is to undermine national identity by promoting sectarian division, regional polarization, and distrust in religious and national institutions. Hostile actors deliberately foster sentiments of marginalization among communities, particularly by reviving historical grievances through digital media, fake literature, and emotionally charged storytelling. Blasphemy related disinformation has become a particularly dangerous tactic. False accusations spread rapidly on social media can incite mob violence, deepen sectarian rifts, and destabilize entire communities. Such disinformation not only undermines public safety but also erodes trust in judicial and religious systems. These campaigns are frequently promoted by anti-state actors seeking to provoke internal chaos under the guise of religious outrage.[15]

Recent events in Kurram District of Khyber Pakhtunkhwa offer a striking example of how 5GW intersects with deep-rooted sectarian tensions. In November 2023, over 80 people were killed in clashes between Sunni and Shia groups, triggered by gunfire on a Shia convoy. Decades of conflict in Kurram, exacerbated by the presence of Sunni extremist groups like TTP, ISIS-K, and Lashkar-e-Jhangvi, have turned the region into a battleground for sectarian dominance. Shia communities report facing extermination campaigns, while Sunni factions blame Shia returnees from the Zainebiyoun Brigade, a militia involved in the Syrian conflict. Experts highlight that the absence of strong governance, political marginalization, and authoritarian security practices have allowed external and internal actors to manipulate these divisions as part of broader 5GW campaigns to fracture Pakistan's ideological unity. These tactics are often exploited by external intelligence operations, particularly by India and Afghanistan, who actively amplify sectarian or ethnic divisions through coordinated disinformation networks and proxy platforms. 5GW actors also weaponize platforms such as BBC, Al Jazeera, and social media to globalize internal issues.

[14] Jahangir, Javeria, and Naheed Bashir. "Fifth Generation Warfare: Response Strategy of Pakistan." *Academic Journal of Social Sciences (AJSS)* 6, no. 2 (2022): 59-76.

[15] Zafar, Zubaida, Sheeba Irfan, and Mubbshar Ali. "Analysing the Role of Religion in Political Structure of Pakistan." *Institute for Strategic Studies, Research and Analysis* (*ISSRA) Papers* 15 (2023).

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Protests, ethnic unrest, and local resistance movements are portrayed as evidence of state oppression and failure. These narratives serve to damage Pakistan's diplomatic credibility and justify international interference, sanctions, or reputational attacks. Furthermore, Islamic ideological coherence a core element of national identity is under attack. Digital campaigns often frame religious orthodoxy as intolerance, painting religious education, institutions, and clerics as regressive or dangerous. Simultaneously, foreign NGOs promote alternative narratives that conflict with traditional Islamic values under the banner of human rights and secular activism.[16]

Anti-state disinformation campaigns also aim to undermine Pakistan's Islamic identity itself. Narratives originating from foreign think tanks, NGOs, and media portray Islamic values as inherently intolerant or incompatible with human rights. These campaigns create a false binary between Islam and progress, gradually alienating younger, liberal-minded citizens from their cultural and religious roots another subtle yet effective dimension of fifth-generation warfare. By framing Pakistan as a country incapable of peaceful co-existence or democratic maturity, 5GW campaigns weaken emotional ties between citizens and the state. The goal is not merely temporary unrest, but a sustained erosion of confidence in the nation's ideological foundation. What makes this threat particularly insidious is its invisibility. Unlike traditional invasions or military standoffs, the damage caused by fifth-generation tactics is psychological, cultural, and long-term. It softens the state from within, reduces its ability to respond to crises, and prepares the ground for future diplomatic or military pressure. As Fifth-Generation Warfare (5GW) blurs the lines between traditional and non-traditional battlefields, it becomes essential to differentiate between the various forms of digital threats operating within this paradigm. In the context of Pakistan, where cyber threats increasingly intersect with national security, public perception, and legal ambiguity, distinguishing between cybercrime, cyber terrorism, and cyber warfare is not only an academic necessity but a policy imperative. Cybercrime refers to illegal activities conducted through digital means, typically for financial or personal gain. This includes identity theft, online fraud, hacking, ransom ware attacks, and unauthorized access to data systems. While cybercrime may not always have political motivation, its consequences can still be severe such as the 2020 ransom ware attack on K-Electric that disrupted services across Karachi. In the 5GW environment, cybercriminals may also be manipulated by external actors, thereby overlapping with broader strategic goals.[17]

Cyber terrorism, on the other hand, is politically or ideologically motivated. It involves using cyberspace to instill fear, disrupt critical infrastructure, or pushing extremist agendas. This may include coordinated attacks on banking systems, digital propaganda by militant groups, or the hacking of government platforms to paralyze governance. Pakistan has been a target of such campaigns, with groups like the Tehrik-i-Taliban Pakistan (TTP) and external networks exploiting social media for recruitment, fundraising, and psychological operations. Cyber warfare represents the highest tire of digital conflict and is often state sponsored. It includes large-scale attacks aimed at weakening a country's defense systems, intelligence networks, or economic infrastructure.

[16] Falki, Sadia Mahmood, and Dure Shahwar Bano. "New Ethnic Identity: Role of Religion and State of Identity in Pakistan." *The Journal of Political Science (JPS)* 37, no. 1 (2019): 143-166.

[17] Akhlaq, Maria. "Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan." *PCL Student Journal of Law* 5, no. 1 (2021): 30-66.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Unlike conventional warfare, cyber warfare is silent, undeclared, and often anonymous. The Stuxnet operation against Iran or the suspected foreign involvement in the PSX and National Bank attacks in Pakistan are examples of how 5GW actors use cyber warfare to achieve strategic disruption without engaging in open conflict. These three categories are not mutually exclusive; they often overlap, especially in hybrid warfare. A cybercriminal act can evolve into cyber terrorism if ideological motives are introduced, and cyber terrorist activity may serve the interests of hostile state actors engaging in cyber warfare. In the absence of clear legal definitions and jurisdictional clarity, Pakistan faces challenges in responding to these threats effectively.[18]

Pakistan Legal Readiness to Combat Fifth-Generation Warfare

The increasing complexity of cyber threats in the era of Fifth-Generation Warfare (5GW) has compelled nations to reconsider and reinforce their digital legal frameworks. Pakistan's legislative response to electronic crimes and hybrid warfare has been primarily constructed through a series of enactments that emerged in response to evolving digital realities. Among these are the Electronic Transactions Ordinance (ETO) 2002, the Prevention of Electronic Crimes Act (PECA) 2016, and the proposed Data Protection Bill of 2018. Each of these represents a significant attempt to regulate cyberspace in an increasingly hostile and technologically advanced environment, though with varying degrees of effectiveness and scope the first formal legislative step came in 2002 with the promulgation of the Electronic Transactions Ordinance (ETO). At the time, Pakistan sought to modernize its financial and administrative infrastructure to accommodate the growing demands of e-commerce, digital communication, and electronic record-keeping. ETO provided legal recognition to electronic documents, digital signatures, and online contracts, creating a framework for transactions in cyberspace. However, ETO was primarily commercial in focus. It was not designed to handle issues of cybercrime, national security, or hostile state behavior in digital environments. With no mechanisms for investigation, prosecution, or penal action against digital wrongdoing, ETO fell short of addressing the emerging cyber threats linked to modern warfare and transnational digital operations.[19]

In response to the inadequacies of ETO and the rising tide of cyber incidents, the government enacted the Prevention of Electronic Crimes Act (PECA) in 2016. This legislation marked a turning point in Pakistan's cyber governance. It was the first law to provide a detailed framework to criminalize various forms of cyber misconduct, including unauthorized access to data, cyber stalking, cyber terrorism, identity theft, electronic fraud, online harassment, hate speech, and the distribution of obscene or false information. PECA also provided statutory authority to the Federal Investigation Agency (FIA) to investigate, prosecute, and manage offenses under its purview, while empowering the judiciary to adjudicate digital cases with special procedures suited to cyberspace. The enactment of PECA filled a significant legislative void. However, it remained largely reactive and framed within the logic of domestic criminal law, making it inadequate for

[18] Hameed, Ishrat, and Syed Asad Ali Naqvi. "An Analysis of the Factors Affecting Cybercrime against Individuals in Pakistan." In *2021 15th International Conference on Open Source Systems and Technologies (ICOSST)*, pp. 1-6. IEEE, 2021.

[19] Ali, Sajjad. "Laws Governing Signatures in Pakistan: An Overview." *UCP Journal of Law & Legal Education* 2, no. 1 (2023): 85-106.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

countering the strategic, transnational, and often state-sponsored threats that characterize 5GW. The law neither classified cross-border cyber-attacks as acts of strategic aggression, nor did it include provisions to prosecute foreign actors who coordinate digital subversion from beyond Pakistan's jurisdiction. High-profile cases such as the ransom ware attack on K-Electric in 2020, the cyber breach at the Federal Board of Revenue (FBR), and the attempted disruption of the National Bank of Pakistan's infrastructure illustrated the vulnerability of Pakistan's cyber ecosystem to hostile foreign influence. Despite the severity of these incidents, PECA lacked both the jurisdictional scope and strategic orientation to deter, investigate, or prosecute cross-border or state-linked actors behind such attacks.[20]

Recognizing the evolving nature of cyber threats, especially those associated with Fifth Generation Warfare (5GW) such as digital propaganda, ideological subversion, and disinformation, the Government of Pakistan introduced comprehensive amendments to PECA on January 29, 2025. These amendments aimed to align the law with hybrid warfare dynamics by expanding its scope, updating key definitions, and establishing mechanisms to monitor and regulate digital behavior more effectively. One of the significant legislative improvements was the inclusion of nine new legal definitions, including terms like 'aspersion', which expanded the scope of defamation-related offenses, and 'complainant', which now allows third-party reporting of certain digital violations. The amendment also introduced a formal definition of 'social media platforms', extending legal liability to natural and legal persons, including companies and web-based service providers. These updates aimed to widen the accountability chain, especially in cases of disinformation or narrative attacks tactics central to 5GW. Additionally, a new Section 26-A was inserted to criminalize the intentional dissemination of false or fake information, reflecting growing concerns over the weaponization of social media. Under this provision, penalties were enhanced to include up to three years imprisonment and fines up to two million rupees, signifying the law's attempt to deter digital destabilization efforts that threaten public order and institutional trust. These amendments represent a strategic legal shift from treating cyber offenses as mere individual crimes to recognizing them as tools of psychological and narrative warfare. By legally framing disinformation as a punishable offense, the state acknowledged its potential to erode national cohesion and security a defining characteristic of 5GW.[21]

One of the most transformative additions in the 2025 amendments was the establishment of new regulatory and judicial institutions. The Social Media Protection and Regulatory Authority (SMPRA) was formed to monitor, regulate, and enforce digital safety standards. The Social Media Protection and Regulatory Authority (SMPRA) was empowered to block or remove offensive content, enlist digital platforms, and cooperate internationally on cyber issues. The authority's role is particularly relevant in 5GW, where narrative control and online propaganda represent strategic weapons. It was accompanied by the formation of Social Media Protection Tribunals (SMPTs) to

[20] Akhlaq, Maria. "Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan." *PCL Student Journal of Law* 5, no. 1 (2021): 30-66.

[21] Iqbal, Muhammad, Samar Raza Talpur, Amir Manzoor, Malik Muneeb Abid, Nazir Ahmad Shaikh, and Sanaullah Abbasi. "The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan." *Siazga Research Journal* 2, no. 4 (2023): 273-282.

THE STUDY OF RELIGION AND HISTORY

ISSN P: 3006-3329

ISSN E: 3006-3337

Vol.3, No.4, 2025

adjudicate disputes, and the creation of a Social Media Complaint Council to streamline citizen grievances regarding unlawful content. Additionally, the National Cyber Crime Investigation Agency (NCCIA) replaced FIA's Cyber Crime Wing, equipped with investigative and forensic authority, including its own digital forensics lab whose findings would now be admissible in court. The agency was mandated to operate with enhanced autonomy and was tasked with coordinating inter-agency cyber defense mechanisms, an area previously weakened by bureaucratic fragmentation. These reforms reflect the state's intent to shift from a reactive, fragmented enforcement model to a more proactive and centralized cyber governance system.[22]

Complementing PECA is the draft Personal Data Protection Bill of 2018, later evolved into the 2023 version. Though still pending formal passage, the updated 2023 Bill represents Pakistan's most direct effort to secure the privacy of citizens' digital information. It seeks to regulate the collection, storage, and processing of personal data by both public and private entities, proposing the establishment of a Data Protection Authority (DPA) tasked with enforcing core data privacy principles such as consent, purpose limitation, data minimization, and the right to erasure. It mirrors global frameworks like the EU's General Data Protection Regulation (GDPR) while incorporating indigenous realities to address Pakistan's vulnerability to 5GW tactics.[23]

In the hybrid warfare context, securing personal data is vital. Surveillance, digital profiling, and unauthorized access to sensitive information are key tools of psychological targeting and electoral manipulation in 5GW. By formalizing protections against such intrusions, the Data Protection Bill seeks to prevent information warfare that exploits personal data at scale. However, the legislative journey remains stalled, slowed by bureaucratic inertia, political sensitivities, and lobbying pressures from influential tech platforms. The urgency for strong data protection became evident with the 2023 NADRA Data Leak Incident, where reports emerged of unauthorized access and potential exposure of citizens' sensitive identity records. The breach not only threatened individual privacy but also posed strategic risks by enabling psychological profiling and targeted disinformation campaigns key components of 5GW. Despite public outcry, accountability remained minimal, exposing gaps in Pakistan's ability to secure its critical data infrastructure in the absence of an enforced data protection regime.[24]

Two recent cases exemplify how the amended PECA 2025 is being operationalized in the context of fifth-generation warfare. In Muzaffargarh, a man was arrested for spreading false blasphemy allegations on social media an act that not only endangered an individual's life but also aimed to provoke communal outrage by exploiting deeply rooted religious sensitivities. This weaponization of religious sentiment through digital platforms aligns closely with the psychological and informational dimensions of 5GW, where chaos is incited without physical confrontation.

[22] Aslam, Muhammad Awais, Abdullah Kanrani, and Muhammad Adil Shehroz. "Regulating Misinformation or Silencing Dissent? A Constitutional Analysis of the PECA Amendments 2025." *The Critical Review of Social Sciences Studies* 3, no. 1 (2025): 1809-1815.

[23] Masudi, Jawed Aziz, and Nasir Mustafa. "Cyber Security and Data Privacy Law in Pakistan: Protecting Information and Privacy in the Digital Age." *Pakistan Journal of International Affairs* 6, no. 3 (2023): 1-11.

[24] Haq, Aly Hassam Ul. "The Right to Privacy & Personal Data Protection: An Analysis of Pakistan's Proposed Personal Data Protection Bill." *UCP Journal of Law & Legal Education* 2, no. 2 (2024): 01-27.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Similarly, in Rawalpindi, a case was registered against an individual for sharing content on Facebook and TikTok that mocked national security institutions and the Chief Minister of Punjab. The material was deemed part of an orchestrated campaign to create public mistrust and incite hatred against the state. In both instances, the use of digital tools to erode social cohesion, challenge institutional authority, and manipulate public perception represents the non-kinetic and subversive tactics central to fifth-generation warfare. These cases demonstrate how PECA 2025 is now being applied not only to curb cybercrimes in the traditional sense but also to counter the broader strategic and ideological challenges posed by hybrid warfare.[25]

Despite the progressive legislative intent behind the enactment of the Prevention of Electronic Crimes Act (PECA) 2016, Pakistan's legal infrastructure remains fundamentally inadequate in responding to the complex threat matrix posed by 5th Generation Warfare (5GW). While PECA provides a statutory framework to tackle cybercrime primarily addressing offenses such as hacking, identity theft, and online harassment it lacks the legal foresight and operational agility to counter multidimensional threats such as hybrid warfare, psychological operations, and foreign-state sponsored disinformation. These tactics, central to the arsenal of 5GW, fall beyond the conventional scope of cybercrime and challenge national security in more subtle and insidious ways. A major conceptual gap stems from PECA's limited definitional scope. The law does not define digital aggression, nor does it incorporate 5GW-specific threats such as strategic disinformation campaigns, hostile foreign surveillance operations (e.g., Pegasus spyware), or persistent malware intrusions targeting critical national infrastructure and psychological stability. Advanced Persistent Threat (APT) groups employing tools like Sunbird and Hornbill to spy on Pakistani officials and defense institutions highlight the asymmetric nature of modern cyber-attacks, yet PECA continues to treat such incidents as isolated criminal offenses rather than integrated acts of information warfare designed to erode state authority from within.[26]

Moreover, PECA Amendment 2025 suffers from structural and jurisdictional limitations that are ill-suited to the transnational nature of contemporary cyber threats. In 5GW scenarios, adversaries often operate beyond national borders, rendering domestic legal mechanisms impotent. Although Pakistan participates in Mutual Legal Assistance Treaties (MLATs), these processes are bureaucratic, time-consuming, and ineffective for the rapid response needed to counter hybrid threats. Additionally, Pakistan's absence from key international frameworks, such as the Budapest Convention on Cybercrime, further isolates its legal apparatus from global cooperative mechanisms. Enforcement inefficacies further aggravate the situation. The Federal Investigation Agency's (FIA) Cyber Crime Wing, formally mandated to implement PECA, suffers from chronic underfunding, a lack of digital forensic capabilities, outdated investigative tools, and acute human resource constraints. As of 2024, with only 350 trained investigators managing over 160,000 cybercrime complaints, case backlogs have become a norm, and conviction rates remain below 1%. This reflects not only procedural stagnation but also fundamental legal ambiguities that allow

[25] Iftikhar, Ifra, Irem Sultana, and Sajjad Ahmad Paracha. "Balancing Act: Pakistan's Quest for Responsible Social Media Regulation." *Pakistan JL Analysis & Wisdom* 3 (2024): 216.

[26] Farrukh, Tehreem. "A Critical Analysis of the Prevention of Electronic Crimes Act (PECA): Legislative Gaps and Enforcement Challenges in Pakistan." *Pakistan Journal of Social Science Review* 4, no. 4 (2025): 1439-1448.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

cyber offenders, particularly those linked to foreign state-sponsored activities, to evade accountability. The 2025 amendments to PECA, though significant in intent, have sparked more controversy than confidence. These reforms introduced new institutional bodies like the Social Media Protection and Regulatory Authority (SMPRA) and the National Cyber Crime Investigation Agency (NCCIA), and expanded criminal liability to include fake news, online dissent, and criticism of state institutions. However, critics argue that these changes skew the law toward controlling speech rather than fortifying digital sovereignty. Legal scholars caution that vague definitions and ambiguous enforcement provisions may enable misuse of authority and erode civil liberties without meaningfully enhancing cyber resilience.[27]

Comparative analysis further underlines Pakistan's challenges. Countries like Bangladesh and Egypt, through the Digital Security Act (2018) and Anti-Cybercrime Law (2021) respectively, have faced similar criticism regarding the weaponization of cyber laws to suppress dissent rather than combat strategic threats. In contrast, models such as Germany's Netzwerkdurchsetzungsgesetz demonstrate how cyber regulations can be structured to balance security needs with human rights protections by emphasizing independent oversight, transparency requirements, and public education initiatives. Pakistan's limited engagement with evolving international cyber norms such as the principles outlined in the Tallinn Manual on International Law Applicable to Cyber Warfare and the recommendations of the UN Group of Governmental Experts (GGE)also reflects a significant normative gap. Without formal integration of these standards, Pakistan lacks clear legal pathways to attribute cyber-attacks, invoke self-defense rights under international law, or participate effectively in international cyber security cooperation forums. Thus, while legislative initiatives like PECA and its 2025 amendments have laid foundational groundwork, critical gaps persist. These gaps leave Pakistan vulnerable not only to cybercriminals but also to sophisticated 5GW tactics aimed at undermining institutional stability, fracturing public trust, and manipulating information ecosystems on a strategic scale. Despite the legislative milestones marked by the enactment of the Prevention of Electronic Crimes Act (PECA) 2016 and its subsequent 2025 amendments, Pakistan continues to face deep-rooted challenges in effectively enforcing cyber laws, particularly in the context of Fifth-Generation Warfare (5GW).[28]

One of the most pressing issues is the severe institutional capacity deficit. The Cyber Crime Wing of the Federal Investigation Agency (FIA), responsible for investigating and prosecuting electronic crimes under PECA, remains under-resourced and overburdened. As of 2024, only 350 investigators were available to process over 160,000 reported cybercrime cases, resulting in a staggering backlog and public disillusionment with the legal process. Most of these cases are delayed well beyond statutory deadlines, while conviction rates remain below 1%. This inadequacy is compounded by a lack of digital forensic expertise, outdated investigative tools, and

[27] Zeb, Mahr Ahmed, and Waleed Rahim. "Cybersecurity in Pakistan: Legal Gaps, Institutional Challenges, and the Need for a Comprehensive National Strategy." *Research Consortium Archive* 3, no. 4 (2025): 1454-1465.

[28] Idrees, Rao Qasim, Naveed Hussain, and Ali Shahid. "Cybercrime Laws in Pakistan: A Critical Analysis of the Prevention of Electronic Crimes Act, 2016." *Journal for Current Sign* 3, no. 4 (2025): 2390-2403.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

minimal inter-agency coordination. Jurisdictional constraints further impede enforcement. Cyber threats emerging in the realm of 5GW such as those tied to foreign disinformation campaigns, coordinated cyber-attacks, and proxy psychological operations often originate from actors operating beyond Pakistan's borders. PECA lacks robust extraterritorial provisions or efficient mechanisms to facilitate the prosecution of foreign actors. Although Pakistan participates in Mutual Legal Assistance Treaties (MLATs), the process remains bureaucratically complex and too slow to address the real-time nature of hybrid threats. Moreover, legal ambiguities in identifying the perpetrators of state-sponsored cyber operations have rendered many foreign-sponsored 5GW attacks untraceable and legally unaccountable. Compared to countries like Israel, which operates a highly integrated cyber defense model through its National Cyber Directorate, Pakistan's jurisdictional and enforcement fragmentation leaves critical vulnerabilities exposed.[29]

From a technological perspective, Pakistan's cyber security enforcement infrastructure is fragmented. Institutions like PakCERT, NR3C, and NTISB operate in isolation, without a unified national command or integrated response mechanism. Provincial and federal agencies often act independently, and coordination is minimal. Most cyber security responses are reactive rather than preventive, focusing on post-incident investigation rather than strategic deterrence or threat neutralization. Moreover, Pakistan's cyber laws still do not mandate essential measures such as routine penetration testing, cyber security audits, or compulsory risk assessments for public and private digital infrastructure. This gap leaves critical sectors including finance, energy, defense, and healthcare highly vulnerable to exploitation by advanced persistent threat (APT) actors using 5GW tactics. Pakistan lacks structured frameworks for public-private sector collaboration, a critical component emphasized globally for effective cyber resilience. Unlike countries where private cyber security firms and state agencies collaborate in real-time threat detection and response, Pakistan's cyber strategy remains overly state-centric, with minimal engagement from private sector innovators and infrastructure owners. The 2025 amendments to PECA aimed to address some of these deficits by creating new enforcement bodies such as the National Cyber Crime Investigation Agency (NCCIA), equipped with its own forensic labs and broader investigative powers. However, concerns remain about the actual implementation of these reforms, given historical trends of institutional inertia, underfunding, and political interference. The NCCIA's potential will remain unrealized unless backed by sustained resource investment, independent oversight, and clear protocols for inter-agency collaboration. While the establishment of NCCIA and related reforms marked a positive legislative step, the operational realities on the ground remain largely unchanged. Without strong political will, capacity building, and strategic inter-agency coordination, the legal advancements introduced in 2025 risk becoming paper reforms with limited impact on Pakistan's actual 5GW defense posture. Thus, despite legislative progress, Pakistan's enforcement architecture continues to exhibit significant structural weaknesses. These enforcement deficits not only weaken Pakistan's cyber resilience but also stand in sharp contrast to the more integrated approaches adopted by other states in countering Fifth-

[29] Kalsoom, Umaira, Aqsa Iram Shahzadi, and Amna Fazail. "Digital Disinformation and Legal Accountability in Pakistan." *Pakistan Journal of Social Science Review* 4, no. 2 (2025): 388-398.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Generation Warfare.[30]

As the threat landscape of Fifth-Generation Warfare (5GW) expands into the cyber and informational domains, states across the globe have evolved their legal frameworks to confront non-kinetic, hybrid threats. Unlike conventional warfare, 5GW exploits disinformation, psychological manipulation, and cyber sabotage to undermine sovereignty, fracture civil cohesion, and destabilize institutions. A comparative analysis of legal responses from India, United States, China, and selected Western nations like Germany and Ukraine offers valuable insights for Pakistan in designing a more adaptive and strategically aligned legal architecture. India's principal cyber legislation, the Information Technology (IT) Act, 2000, along with its 2021 IT Rules, has undergone continuous amendments to regulate digital conduct, disinformation, and state security concerns. The IT Act, particularly under Section 66F, addresses cyber terrorism and grants authorities' power to intercept digital communication in the name of national interest. Complementing this, India's Unlawful Activities (Prevention) Act (UAPA) allows digital content associated with terrorism or separatism to be legally defined as unlawful, enabling prosecution and takedown. India's counter-5GW strategy came into sharper focus during the 2021 farmer protests, where the government directed Twitter and other platforms to block over 1,100 accounts accused of pushing pro-Khalistan propaganda and spreading misleading narratives such as "#ModiPlanningFarmersGenocide." Indian intelligence identified many of these accounts as linked to Pakistan and other external actors, portraying the protests as a human rights crisis to international audiences. These actions demonstrated India's use of digital law fare to counter hybrid threats.[31]

Moreover, India's enactment of the Digital Personal Data Protection Act, 2023 further strengthened its cyber security regime by regulating personal data management and enhancing state oversight over digital platforms. Formal notices issued under IT Rules (2021) compelled platforms to comply or face legal penalties, including loss of intermediary protections. These actions underscore India's use of digital law fare to combat 5GW disinformation while preserving domestic order. In addition, India's National Cyber Coordination Centre (NCCC) and state surveillance agencies continue to track separatist narratives and extremist content. The government has collaborated with global platforms to de-platform pro-Khalistan actors, treating these narratives as foreign-sponsored psychological warfare. Such comprehensive responses spanning legislation, real-time cyber forensics, and diplomatic engagement exemplify India's integrated strategy in neutralizing 5GW threats through legal mechanisms.[32]

The ongoing conflict between Russia and Ukraine exemplifies the complex dynamics of Fifth-Generation Warfare (5GW), characterized by a fusion of cyber-attacks, disinformation campaigns, and psychological manipulation. Since 2014, Russia has aggressively employed 5GW tactics to

[30] Saleem, Hobashia, Junaid Jan, and Azzalfa Areej. "Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges." *Society, Law and Policy Review* 1, no. 1 (2022): 10-22.

[31] Fernandes, Yohan, and Nasr Abosata. "Analyzing India's Cyber Warfare Readiness and Developing a Defense Strategy." *arXiv preprint arXiv:2406.12568* (2024).

[32] Amal Chandra, C. "Strengthening India's Cybersecurity and Data Privacy Landscape: A Comprehensive Overview." *Indian Journal of Public Administration* 70, no. 3 (2024): 466-478.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

destabilize Ukraine, ranging from the dissemination of fabricated narratives through troll farms and state-sponsored media to devastating cyber offensives such as the NotPetya malware attack in 2017, which disrupted banks, government services, and energy infrastructure across Ukraine. In response, Ukraine has adopted a dual-track approach that combines international support with domestic legal reforms to build resilience against these hybrid threats. Internationally, Ukraine has collaborated closely with NATO and the European Union to enhance its cyber defense capabilities. NATO has provided technical assistance, intelligence sharing, and cyber security training to Ukrainian agencies, while the EU has funded programs aimed at countering disinformation, supporting digital literacy, and establishing independent fact-checking bodies. These efforts have helped Ukraine rapidly develop institutional defenses against foreign psychological and cyber warfare. Concurrently, Ukraine has undertaken significant legal reforms to assert its digital sovereignty and respond to 5GW threats through legislative means. In 2020, it enacted a revised Law on the basic principles of cyber security, which mandates cyber resilience standards for critical infrastructure and formalizes the responsibilities of state institutions in national cyber security. The law also encourages cooperation between public and private sectors in the monitoring, prevention, and prosecution of cyber-enabled threats. In addition, Ukrainian authorities have initiated legal action against foreign propaganda campaigns and adopted stricter media regulations to deter the spread of disinformation linked to external state actors. This integrated strategy rooted in both legal development and strategic alliances highlights Ukraine's evolving capacity to resist non-kinetic aggression. Unlike countries with long-established cyber security doctrines, Ukraine's experience underscores the importance of adaptability, legal innovation, and international cooperation in countering modern warfare tactics that seek to weaken a state from within without firing a single shot.[33]

Germany's cyber security approach emphasizes safeguarding democratic values while strengthening resilience against hybrid threats. The Network Enforcement Act (NetzDG) of 2017 mandates that social media platforms swiftly remove unlawful content, such as disinformation and extremist propaganda, while ensuring judicial oversight to prevent abuses of state power. Additionally, the Federal Office for Information Security (BSI) coordinates national cyber security operations, and the country's commitment to the European Union's General Data Protection Regulation (GDPR) reflects a high standard for privacy protections. Germany's system was notably effective during the 2017 federal elections, when the country was targeted by foreign disinformation campaigns seeking to influence electoral outcomes. German authorities responded with rapid enforcement actions under NetzDG, widespread public education efforts about fake news, and enhanced cyber security measures for political entities. For Pakistan, Germany's experience underscores the possibility of building a robust cyber defense system that simultaneously upholds transparency, human rights, and strategic resilience against 5GW tactics.[34]

[33] Nair, Sreejith Sreekandan. "Digital Warfare: Cyber security Implications of the Russia-Ukraine Conflict." *International Journal of Emerging Trends in Computer Science and Information Technology* 4, no. 4 (2023): 31-40.

[34] Susila, Muh Endriyo, and Andi Agus Salim. "Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany." *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 11, no. 1 (2024): 2.

THE STUDY OF RELIGION AND HISTORY

ISSN P: 3006-3329

ISSN E: 3006-3337

Vol.3, No.4, 2025

The United States maintains a multi-layered cybersecurity strategy grounded in legislation, multi-agency coordination, and strong public-private partnerships. Agencies like the Cyber-Security and Infrastructure Security Agency (CISA), the NSA Cyber-Security Directorate, and the FBI Cyber Division operate under a unified national cyber security framework. The "Defend Forward" doctrine, introduced through the 2018 Department of Defense Cyber Strategy, emphasizes proactive disruption of cyber threats before they escalate. The Solar Winds cyber-attack in 2020, attributed to Russian actors, exposed vulnerabilities across federal and private networks. The U.S. responded comprehensively, combining legal sanctions, operational countermeasures, and private-sector mobilization to contain the breach. Rather than viewing it solely as a criminal act, the U.S. treated the incident as a national security threat, demonstrating the strength of its integrated cyber defense system. For Pakistan, the American model highlights that a credible response to 5GW threats requires not just laws but coordinated institutional action, operational readiness, and active partnerships with the private sector.[35]

China's cyber security governance is built on the principle of "Cyber Sovereignty," granting the state full control over digital infrastructure and information flows. Through the Cyber Security Law of 2017 and the Data Security Law of 2021, China mandates data localization, real-name internet registration, and strict regulation of online activities. This approach was visibly enforced during the 2020–2021 crackdown on tech giants like Alibaba and Didi Chuxing, where authorities cited data security and national sovereignty concerns to regulate and penalize companies posing perceived risks. China's readiness to operationalize its cyber laws reflects a strategic focus on securing critical digital assets against hybrid threats. For Pakistan, China's model emphasizes the need for protecting strategic data and national digital infrastructure; however, it also warns against the risks of over-centralization, which could stifle innovation and international engagement. In the evolving landscape of Fifth Generation Warfare (5GW), cyber warfare and electronic crimes have emerged as strategic tools that transcend physical borders and conventional battlefields. Unlike traditional warfare, 5GW leverages psychological operations, information distortion, and digital sabotage to undermine national stability, manipulate public opinion, and disrupt essential infrastructure. Given the transnational and technologically advanced nature of such threats, international legal instruments play a pivotal role in guiding state behavior, enhancing accountability, and enabling cooperation in cyberspace.[36]

While Pakistan has established a domestic legal framework through instruments such as PECA 2016, the absence of integration with international standards significantly limits its ability to counter hybrid and cross-border cyber threats effectively. The Tallinn Manual on International Law Applicable to Cyber Warfare stands as a foundational interpretive document that outlines how established principles of international law apply to cyber operations. It provides legal clarity on complex issues such as state sovereignty in cyberspace, the threshold of cyber-attacks qualifying as a use of force, and the conditions under which a state may exercise its right to self-defense.

[35] Lawson, Sean. "War by Any Other Name: A Short History of the Idea of Cyber-Warfare in the United States." In *Research Handbook on Cyber-Warfare*, pp. 15-33. Edward Elgar Publishing, 2024.

[36] Tan, Er-Win, and Sofiya Sayankina. "Cyberwarfare and the Weaponization of Information in US–China 21st-Century Geostrategic Rivalry." *Pacific Focus* 38, no. 2 (2023): 180-209.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Specifically, the Tallinn Manual deals with state-sponsored disinformation campaigns, cyber espionage, ransom ware attacks that cause physical or financial damage, and coordinated digital sabotage against critical infrastructure. Although the Manual is non-binding, it offers actionable guidelines on state responsibility, due diligence, and legal attribution tools crucial for responding to 5GW tactics. Countries like India, though not a formal adopter, has used its conceptual framework to shape legal discourse and policymaking. Pakistan, however, has yet to formulate a formal stance on the Tallinn Manual, reflecting a normative gap in its approach to cyber warfare under 5GW.[37]

Another essential framework is the United Nations Charter**,** particularly Articles 2(4) and 51, which have been interpreted to include cyber-attacks within the broader legal definitions of use of force and self-defense. Cyber operations that disable hospitals, breach defense systems, paralyze communication infrastructure, or manipulate electoral processes fall within the realm of Article 2(4), especially when they threaten peace and security. The UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) have further articulated norms of responsible state behavior, calling for abstention from cyber activities that violate the sovereignty of other states or disrupt critical civilian infrastructure. These provisions are directly applicable to 5GW phenomena such as election interference, psychological warfare through disinformation, and systemic cyber sabotage. Countries like India actively participate in these UN forums and have begun adapting these principles domestically. Pakistan, on the other hand, lacks explicit policy integration of these norms, which constrains its ability to respond lawfully to international cyber provocations rooted in 5GW.[38]

The Budapest Convention on Cybercrime, though not a warfare-oriented instrument, addresses many electronic crimes that form the technical and legal foundation of 5GW operations. It criminalizes unauthorized access, data breaches, identity theft, digital fraud, malware dissemination, and child exploitation on digital platforms. These crimes are often used strategically in 5GW to erode institutional trust, extract sensitive data, blackmail public officials, or destabilize financial systems. The Convention also facilitates international cooperation in cybercrime investigations through mechanisms like mutual legal assistance, cross-border data sharing, and digital forensics. While India is a signatory aligns closely with its provisions, Pakistan remains outside the Convention, citing sovereignty concerns. However, selective adoption of its procedural tools or alignment through regional cooperation mechanisms such as through SCO or OIC cyber security frameworks could significantly enhance Pakistan's legal capacity to counter cross-border electronic crimes within a 5GW context.[39]

---

[37] Gul, Seema, Wasmiya Malik, and Gohar Masood Qureshi. "Cyber Security and Sovereignty: The Role of International Law in Governing State Behavior in Cyberspace." *Policy Journal of Social Science Review* 3, no. 5 (2025): 121-135.

[38] Usman, Hazrat, and Showkat Ahmad Mir. "Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2 (4) of the UN Charter." *Global Legal Studies Review* 8, no. 2 (2023): 16-26.

[39] Campina, Ana, and Carlos Rodrigues. "Cybercrime and the Council of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation." In *The Book of Full Papers-7th International Zeugma Conference on Scientific Researches*, vol. 1, no. 1, pp. 112-123. IKSAD, 2022.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

The Geneva Conventions, though originally formulated to regulate kinetic warfare, have gained significant relevance in the digital battlefield of Fifth Generation Warfare. Under international humanitarian law, the Geneva Conventions particularly Protocol I and Article 36 mandate the principles of distinction, proportionality, and precaution. These principles are crucial when cyber operations are directed at or impact civilian populations and essential services. In 5GW, where non-kinetic tactics like cyber sabotage are intentionally used to blur the line between civilian and military targets, these legal norms serve as ethical boundaries. For instance, cyber-attacks targeting hospitals, public health systems, water supply networks, or national energy grids tactics increasingly witnessed in modern cyber conflicts can be considered violations of the Geneva Conventions if they result in disproportionate harm to civilians relative to their military utility. While several European Union states have begun to adapt these humanitarian standards to their cyber doctrines, Pakistan has yet to adopt or operationalize the Geneva principles in its national cyber security or military policies, leaving a critical ethical and legal gap in its approach to 5GW.[40] Customary International Law further reinforces the international legal order in cyberspace by codifying widely accepted principles such as non-intervention, proportionality, sovereignty, due diligence, and attribution. These principles directly apply to cyber operations that attempt to manipulate democratic institutions, infiltrate defense databases, or incite unrest through fake news and psychological warfare. Such operations, while falling short of kinetic force, are core tactics of 5GW. Many Western countries, alongside India, have formally recognized and operationalized these norms through domestic legislation and judicial interpretation. Pakistan, however, has yet to formally align its national law with these emerging principles, limiting its ability to invoke or enforce them in international forums or during bilateral disputes related to cyber incursions.[41]

Conclusions and Recommendations

Fifth-Generation Warfare (5GW) is a shift in conflict, replacing traditional military engagements with cyber-attacks, disinformation, psychological manipulation, and ideological subversion. This thesis examines the impact of 5GW in Pakistan, highlighting how digital vulnerabilities, societal divisions, and information warfare are strategically exploited to destabilize the nation without kinetic confrontation. It identifies weaknesses in Pakistan's capacity to address the complex threats posed by 5GW, including the Pegasus spyware scandal and K-Electric ransom ware attack. Pakistan's legal response to cyber threats, based on the Prevention of Electronic Crimes Act (PECA) 2016 and its 2025 amendments, is reactive, fragmented, and insufficient to counter 5GW threats. PECA 2016 lacks provisions for strategic disinformation, psychological operations, and hostile foreign digital influence. The implementation of cyber security policies is hindered by limited institutional coordination, inadequate technical resources, jurisdictional challenges, and specialized training for sophisticated cyber warfare techniques.

Pakistan needs to shift from a purely cybercrime-focused approach to a more integrated cyber defense and hybrid warfare strategy, focusing on proactive threat hunting, public-private sector

[40] Sutherland, Iain, Konstantinos Xynos, Andrew Jones, and Andrew Blyth. "The Geneva Conventions and Cyber-Warfare: A Technical Approach." *The RUSI Journal* 160, no. 4 (2015): 30-39.

[41] Polański, Paul Przemysław. "Cyberspace: A New Branch of International Customary Law?." *Computer Law & Security Review* 33, no. 3 (2017): 371-381.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

collaboration, national cyber commands, societal resilience building, and international cooperation. Pakistan's unique socio-political context is further exacerbated by the lack of comprehensive data protection legislation, which exacerbates vulnerability to digital profiling, surveillance, and psychological targeting, central tactics of 5GW.

The research highlights the strategic use of Pakistan's internal fault lines through disinformation campaigns and psychological manipulation, posing a long-term threat to its sovereignty. This involves weaponizing historical grievances, promoting extremist narratives, and fostering distrust, aiming to erode the state's internal coherence and external credibility. This research emphasizes the need for Pakistan to recognize 5GW as a distinct national security threat, addressing gaps in current laws and strategies. It proposes reforms such as updating PECA to criminalize strategic disinformation and psychological operations, establishing a Unified National Command for Cyber and Hybrid Warfare, bridging civil-military gaps, strengthening institutional technical capacity, enforcing strict data protection measures, and building societal immunity through digital literacy and national narrative reinforcement.

Pakistan must adopt a coherent, multidimensional strategy to defend against Fifth-Generation Warfare (5GW) in the 21st century. Failure to adapt risks adversaries exploiting Pakistan's digital vulnerabilities and societal fissures, weakening national unity and resilience. Integrating legal, strategic, institutional, and societal reforms is crucial.

To ensure a unified national response to emerging non-kinetic threats, it is imperative that Pakistan formally declare Fifth-Generation Warfare (5GW) a national security threat and incorporate it into the country's strategic framework. The National Security Division should include 5GW as a distinct category in its policy framework. Civil-military agencies must collaboratively draft a 5GW Response Doctrine with defined protocols and inter-agency coordination. This unit should monitor real-time digital threats, psychological campaigns, and hostile information operations. It should operate under a centralized civilian-military command, with technical experts, media analysts, and legal oversight. Strengthen DG ISPR and Ministry of Information’s communication departments with proactive narrative-building capacity. Promote public education campaigns to counter digital propaganda, misinformation, and false flag operations. Collaborate with allies like China, Turkey, and Malaysia to establish joint cyber defense alliances. Engage with international forums (e.g., Tallinn Manual working groups, UN GGE) to formalize responses to non-kinetic aggression and disinformation warfare. These policy steps will provide the foundational recognition and direction needed to effectively counter the broad-spectrum threats of Fifth-Generation Warfare. Recognizing 5GW as a strategic threat is the first and most crucial step in shaping Pakistan’s national resilience across military, legal, and societal domains.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

References

Abawe, Zulfia. "A Relational Analysis of the Pashtun Tahafuz Movement (PTM) in Pakistan." *Ethnopolitics* (2026): 1-22.

Aslam, Muhammad Awais, Abdullah Kanrani, and Muhammad Adil Shehroz. "Regulating Misinformation or Silencing Dissent? A Constitutional Analysis of the PECA Amendments 2025." *The Critical Review of Social Sciences Studies* 3, no. 1 (2025): 1809-1815.

Amal Chandra, C. "Strengthening India's Cybersecurity and Data Privacy Landscape: A Comprehensive Overview." *Indian Journal of Public Administration* 70, no. 3 (2024): 466-478.

Ali, Sajjad. "Laws Governing Signatures in Pakistan: An Overview." *UCP Journal of Law & Legal Education* 2, no. 1 (2023): 85-106.

Akhlaq, Maria. "Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan." *PCL Student Journal of Law* 5, no. 1 (2021): 30-66.

Adamson, A., & Snyder, M. (2017). The Challenges of Fifth-Generation Transformation. *The Rusi Journal*, *162*(4), 60-66.

Campina, Ana, and Carlos Rodrigues. "Cybercrime and the Council of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation." In *The Book of Full Papers-7th International Zeugma Conference on Scientific Researches*, vol. 1, no. 1, pp. 112-123. IKSAD, 2022.

Farrukh, Tehreem. "A Critical Analysis of the Prevention of Electronic Crimes Act (PECA): Legislative Gaps and Enforcement Challenges in Pakistan." *Pakistan Journal of Social Science Review* 4, no. 4 (2025): 1439-1448.

Fernandes, Yohan, and Nasr Abosata. "Analyzing India's Cyber Warfare Readiness and Developing a Defense Strategy." *arXiv preprint arXiv:2406.12568* (2024).

Falki, Sadia Mahmood, and Dure Shahwar Bano. "New Ethnic Identity: Role of Religion and State of Identity in Pakistan." *The Journal of Political Science (JPS)* 37, no. 1 (2019): 143-166.

Gul, Seema, Wasmiya Malik, and Gohar Masood Qureshi. "Cyber Security and Sovereignty: The Role of International Law in Governing State Behavior in Cyberspace." *Policy Journal of Social Science Review* 3, no. 5 (2025): 121-135.

Haq, Aly Hassam Ul. "The Right to Privacy & Personal Data Protection: An Analysis of Pakistan's Proposed Personal Data Protection Bill." *UCP Journal of Law & Legal Education* 2, no. 2 (2024): 01-27.

Hameed, Ishrat, and Syed Asad Ali Naqvi. "An Analysis of the Factors Affecting Cybercrime against Individuals in Pakistan." In *2021 15th International Conference on Open Source Systems and Technologies (ICOSST)*, pp. 1-6. IEEE, 2021.

Idrees, Rao Qasim, Naveed Hussain, and Ali Shahid. "Cybercrime Laws in Pakistan: A Critical Analysis of the Prevention of Electronic Crimes Act, 2016." *Journal for Current Sign* 3, no. 4 (2025): 2390-2403.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Iftikhar, Ifra, Irem Sultana, and Sajjad Ahmad Paracha. "Balancing Act: Pakistan's Quest for Responsible Social Media Regulation." *Pakistan JL Analysis & Wisdom* 3 (2024): 216.

Iqbal, Muhammad, Samar Raza Talpur, Amir Manzoor, Malik Muneeb Abid, Nazir Ahmad Shaikh, and Sanaullah Abbasi. "The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the Challenges in Pakistan." *Siazga Research Journal* 2, no. 4 (2023): 273-282.

Jahangir, Javeria, and Naheed Bashir. "Fifth Generation Warfare: Response Strategy of Pakistan." *Academic Journal of Social Sciences (AJSS)* 6, no. 2 (2022): 59-76.

Kalsoom, Umaira, Aqsa Iram Shahzadi, and Amna Fazail. "Digital Disinformation and Legal Accountability in Pakistan." *Pakistan Journal of Social Science Review* 4, no. 2 (2025): 388-398.

Khan, A. M. (2025). 5th Generation Warfare and the Erosion of Traditional State Power: Analyzing Non-Kinetic Strategies in Modern Conflict. *International Journal of Social Sciences Bulletin*, *3*(3), 915-924.

Krishnan, A. (2024). *Fifth Generation Warfare: Dominating the Human Domain*. Routledge.

Krishnan, A. (2022). Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict. *Journal of Strategic Security*, *15*(4), 14-31.

Kelshall, C. M. (2022). Fifth Generation Warfare? Violent Transnational Social Movements as Security Disruptors. in *Disruption, Ideation and Innovation for Defence and Security* (pp. 269-298). Cham: Springer International Publishing.

Kamboh, Muhammad Khalique, Ghulam Mustafa, and Muhammad Fazal Rasul. "5th Generation Warfare and Issues of National Integration in Pakistan." *Pakistan Social Sciences Review* 5, no. 1 (2021): 802-814.

Lawson, Sean. "War by Any Other Name: A Short History of the Idea of Cyber-Warfare in the United States." In *Research Handbook on Cyber-Warfare*, pp. 15-33. Edward Elgar Publishing, 2024.

Mahmood, Sohail. "A Tumultuous Election Day in Pakistan: The 2024 General Election Turmoil." *International Policy Digest* (2024).

Masudi, Jawed Aziz, and Nasir Mustafa. "Cyber Security and Data Privacy Law in Pakistan: Protecting Information and Privacy in the Digital Age." *Pakistan Journal of International Affairs* 6, no. 3 (2023): 1-11.

Nair, Sreejith Sreekandan. "Digital Warfare: Cyber security Implications of the Russia-Ukraine Conflict." *International Journal of Emerging Trends in Computer Science and Information Technology* 4, no. 4 (2023): 31-40.

Nawaz, Adnan, Muhammad Zeeshan, and Sufyan Akhlaq. "Fifth-Generation Warfare: A Quagmire and Fiasco to National Solidity of Pakistan." *South Asian Studies* 38, no. 01 (2023): 53-72.

Nadeem, Muhammad Ashraf, Ghulam Mustafa, and Allauddin Kakar. "Fifth Generation Warfare and its Challenges to Pakistan." *Pakistan Journal of International Affairs* 4, no. 1 (2021): 216-230.

THE STUDY OF RELIGION AND HISTORY

Vol.3, No.4, 2025

ISSN P: 3006-3329

ISSN E: 3006-3337

Patel, A. (2019). Fifth-Generation Warfare and the Definitions of Peace. *The Journal of Intelligence, Conflict, and Warfare*, *2*(2), 15-28.

Polański, Paul Przemysław. "Cyberspace: A New Branch of International Customary Law?." *Computer Law & Security Review* 33, no. 3 (2017): 371-381.

Qureshi, W. A. (2019). Fourth-and Fifth-Generation Warfare: Technology and Perceptions. *San Diego International Law Journal*, *21*, 187.

Susila, Muh Endriyo, and Andi Agus Salim. "Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany." *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)* 11, no. 1 (2024): 2.

Saleem, Hobashia, Junaid Jan, and Azzalfa Areej. "Cyber Crimes Trends in Pakistan: Analyzing the Legal Framework and Enforcement Challenges." *Society, Law and Policy Review* 1, no. 1 (2022): 10-22.

Sutherland, Iain, Konstantinos Xynos, Andrew Jones, and Andrew Blyth. "The Geneva Conventions and Cyber-Warfare: A Technical Approach." *The RUSI Journal* 160, no. 4 (2015): 30-39.

Tan, Er-Win, and Sofiya Sayankina. "Cyberwarfare and the Weaponization of Information in US–China 21st-Century Geostrategic Rivalry." *Pacific Focus* 38, no. 2 (2023): 180-209.

Usman, Hazrat, and Showkat Ahmad Mir. "Beyond Conventional War: Cyber Attacks and the Interpretation of Article 2 (4) of the UN Charter." *Global Legal Studies Review* 8, no. 2 (2023): 16-26.

Zafar, Zubaida, Sheeba Irfan, and Mubbshar Ali. "Analysing the Role of Religion in Political Structure of Pakistan." *Institute for Strategic Studies, Research and Analysis* (*ISSRA) Papers* 15 (2023).