Asian journal of International Peace and Security (AJIPS)

ISSN-e: 2707-8809

Vol. 8, No. 3, (2024, Autumn), 39-57

Fifth Generation Warfare and Cyber Conflict: Pakistan's Vulnerability to Digital Terrorism

Saeed Ahmed[1]

Abstract:

The rise of digital terrorism and the increasing use of cyber warfare techniques pose significant threats to Pakistan's national security. This research explores the evolving landscape of Fifth Generation Warfare (5GW) and its implications for state stability, focusing on the role of disinformation, cyber espionage, and extremist digital mobilization. The core issue under examination is how state and non-state actors leverage digital platforms to manipulate public perception, destabilize institutions, and undermine national security frameworks. To analyze these threats, the study applies Hybrid Warfare Theory (HWT) and Cyber Conflict Theory (CCT) as conceptual frameworks. The research employs a qualitative methodology, incorporating a thematic analysis of policy reports, government records, cybersecurity assessments, and expert interviews. Additionally, a comparative approach is used to assess how internal and external cyber threats interact, particularly within the Pakistan-India geopolitical rivalry and the role of transnational terrorist networks in online radicalization. Findings reveal critical gaps in Pakistan's cybersecurity policies, institutional preparedness, and civil-military coordination, highlighting vulnerabilities in both digital governance and crisis response mechanisms. The study concludes that a robust national cybersecurity strategy, enhanced cyber diplomacy, and AI-driven threat detection mechanisms are essential for mitigating digital terrorism.

INTRODUCTION

In the modern security landscape, warfare has evolved beyond traditional military confrontations. Fifth Generation Warfare (5GW) represents a shift from conventional battlefields to the digital domain, where cyber tools, disinformation campaigns, and psychological manipulation are employed to influence societies and destabilize states. This transformation has created new vulnerabilities for countries like Pakistan, where cyber threats intersect with political instability, regional conflicts, and internal security challenges (Hoffman, 2017; Nisar, 2020).

Digital terrorism—the use of cyber-based tactics to spread extremist propaganda, manipulate public perception, and weaken institutions—has become a pressing national security concern. Political actors, terrorist organizations, and foreign intelligence agencies increasingly exploit digital platforms to achieve strategic, ideological, and geopolitical objectives (Yasin, 2021). The widespread use of social media, artificial intelligence (AI), and algorithmic manipulation has blurred the line between information warfare and cybercrime, making it difficult for states to

[1] PhD Scholar, Department of International Relations, Preston University, Islamabad, Pakistan. Email: sminhas07@gmail.com

respond effectively. As Buchanan (2020) notes, "cyber conflicts do not merely supplement traditional warfare; they redefine the very nature of state security."

This research aims to analyze the role of digital terrorism within the 5GW paradigm and its impact on Pakistan's national security architecture. It will also examine how both state and non-state actors employ cyber tools for political and ideological manipulation. By evaluating Pakistan's cybersecurity readiness, the research will help identify key institutional and legislative gaps that hinder an effective response to cyber threats. It plans to propose strategic recommendations for strengthening Pakistan's security framework against digital terrorism and cyber warfare.

Using Hybrid Warfare Theory (HWT) and Cyber Conflict Theory (CCT) as conceptual lenses, this study investigates how both state and non-state actors leverage cyberspace to challenge national security paradigms (Rattray & Healey, 2011). By addressing these dimensions, the study contributes to the broader discourse on digital sovereignty, cyber governance, and the role of emerging technologies in modern conflict. As Krishnan (2022) asserts, "The battlefield of the future will not be fought with conventional weapons but with data, narratives, and the power to control perception." Understanding these dynamics is crucial for developing a robust national security strategy that aligns with the evolving nature of cyber threats.

RESEARCH METHODOLOGY

The research applies a qualitative methodology, drawing from policy documents, cybersecurity reports, case studies, and expert interviews to assess Pakistan's vulnerabilities. It employs thematic analysis of policy reports, government records, cybersecurity assessments, and expert interviews. Additionally, a comparative approach is used to assess how internal and external cyber threats interact, particularly within the Pakistan-India geopolitical rivalry and the role of transnational terrorist networks in online radicalization. Through this analysis, the study aims to provide actionable insights into strengthening Pakistan's cybersecurity framework, enhancing institutional resilience, and formulating policies to counter digital terrorism effectively.

THEORETICAL UNDERPINNING

The study of digital terrorism within the broader landscape of Fifth Generation Warfare (5GW) requires a theoretical foundation that explains both the strategic intent behind cyber conflicts and their operational execution. This research is grounded in Hybrid Warfare Theory (HWT) and Cyber Conflict Theory (CCT), two frameworks that collectively provide insight into how cyber tools, information manipulation, and non-conventional tactics are deployed to achieve political, military, and ideological objectives (Mumford, 2013; Hoffman, 2017).

In this context, the Independent Variables (IVs) represent the mechanisms used in digital warfare—cyber-attacks, disinformation campaigns, economic coercion, and non-state actor involvement—while the Dependent Variables (DVs) reflect the outcomes of these efforts, such as national security destabilization, institutional vulnerability, public perception shifts, and geopolitical tensions (Krishnan, 2022).

Hybrid Warfare Theory (HWT)

HWT explains how state and non-state actors blend conventional and unconventional tactics to weaken an adversary. Unlike traditional warfare, which relies on military engagements, hybrid

conflicts operate in the grey zone between war and peace, leveraging cyber capabilities, disinformation, and irregular warfare to create confusion and erode state authority (Hoffman, 2017).

The key Independent Variables (IVs) in HWT include;

- Conventional Forces: The use of regular military operations in coordination with cyber warfare and digital misinformation to weaken the opponent.
- Irregular Tactics: The employment of non-state actors, insurgent groups, or proxy forces to destabilize governance and fuel internal conflicts (Mumford, 2013).
- Cyber Warfare: Targeted attacks on digital infrastructure, hacking of sensitive data, and information disruption to cripple an adversary's communication and decision-making systems (Denning, 2001).
- Information Warfare: The spread of propaganda, fake news, and psychological operations designed to manipulate public perception and erode trust in institutions.
- Economic and Political Pressure: The strategic use of economic sanctions, trade restrictions, and political maneuvering to coerce or weaken adversaries without direct military confrontation.

The Dependent Variables (DVs) resulting from these tactics include;

- National Security Instability: The weakening of state authority and crisis in governance due to cyber-enabled hybrid warfare.
- Institutional Vulnerabilities: Gaps in legislative and security frameworks that allow hostile entities to exploit cyber loopholes.
- Shifts in Public Perception: The success of disinformation campaigns in reshaping national narratives, creating division, or fueling public dissent.
- Regional Geopolitical Tensions: The destabilizing effects of cyber-enabled hybrid warfare on Pakistan's relations with neighbouring states, particularly in the context of India and transnational cyber threats.

Cyber Conflict Theory (CCT) and its Key Variables

While HWT explains the broader integration of digital and conventional tactics, Cyber Conflict Theory (CCT) focuses specifically on the role of cyber tools in modern warfare. This theory posits that cyberspace is an independent battleground where states and non-state actors engage in offensive and defensive cyber operations to gain strategic advantages (Kello, 2017).

The Independent Variables (IVs) in CCT include;

- Cyber Offense: The use of hacking, malware, phishing, and ransomware attacks to compromise adversary networks, steal classified data, or disrupt digital infrastructure (Clarke & Knake, 2010).
- Cyber Defence: The deployment of firewalls, encryption, AI-driven threat detection, and cybersecurity protocols to protect state and private networks from cyber intrusions.
- Actors: Various entities, including state-sponsored cyber units, independent hacker groups, terrorist organizations, and cybercriminal networks, all compete for digital dominance (Buchanan, 2020).
- Targeting: The selection of critical assets—government databases, military communication networks, financial institutions, and key infrastructure—to achieve political, economic, or military objectives.

- Cyber Espionage: The act of stealing classified government data, intellectual property, or military secrets through covert digital means to gain geopolitical advantages (Rattray & Healey, 2011).
- Attribution and Legal Frameworks: The challenges of identifying perpetrators of cyberattacks, enforcing accountability, and developing global norms to regulate cyber conflicts.

The Dependent Variables (DVs) emerging from these factors include;

- Digital Sovereignty Threats: The compromise of national security due to cyber intrusions targeting state institutions and key infrastructure.
- Economic Disruptions: The financial consequences of cyberattacks, including ransomware threats, financial fraud, and targeted economic sabotage.
- Erosion of Trust in Digital Governance: Public skepticism towards cybersecurity policies and state control over digital platforms, especially when cyber threats remain unresolved.
- Cyber Arms Race and International Conflicts: The escalation of state-sponsored cyber operations and retaliatory cyber warfare leading to worsened geopolitical relations.

Application to Pakistan's National Security Context

By integrating HWT and CCT, this study examines how Pakistan's cybersecurity vulnerabilities stem from both hybrid and cyber conflict strategies deployed by state and non-state actors. In the context of Pakistan Hybrid Warfare, as Nadeem et al., (2021) portray manifests in disinformation campaigns, online extremist recruitment, and the geopolitical use of cyber tools by foreign adversaries. Cyber Conflict is evident in state-backed hacking attempts, infrastructure breaches, and economic cyber warfare targeting financial systems.

This research will provide a comprehensive analysis of Pakistan's digital security landscape by examining its national security architecture, its vulnerabilities in light of its cyber regulations, enforcement of cybersecurity laws, and institutional coordination. Eventually, the study aims to propose policy-driven solutions to strengthen cybersecurity governance, cyber deterrence mechanisms, and digital resilience in an era of AI-driven hybrid and cyber warfare.

LITERATURE REVIEW: BRIDGING THEORETICAL AND OPERATIONAL GAPS

The study of 5GW and hybrid wars as presented in modern scholarship implies a revolutionary transformation of modern warfare thinking and action, especially if situated against the background of AI-driven digital technology. Unlike previous generations that focused on traditional military conflict, 5GW is defined by decentralized actors leveraging technology to influence public opinion and discredit adversaries without resorting to traditional combat. 5GW has been referred to as a "war of information and perception," with the battlefield being extended to cyberspace and social media platforms (Abbot, 2022). The ambiguity of the nature of 5GW makes its characterization difficult; it involves a wide array of tactics that can be employed simultaneously by state and non-state actors (Hoffman, 2017).

Hybrid warfare is the confluence of conventional and unconventional strategies, blending conventional military power with psychological warfare and cyber warfare (Nisar, 2020). The term gained popularity after the 2006 Israel-Hezbollah war when both nations applied a combination of conventional military strategy and asymmetrical means to achieve their purposes (Schaub et al., 2017). Hybrid warfare is more than a tactical approach; it is a strategic framework that takes

advantage of loopholes in different spheres—political, economic, social, and informational (Krishnan, 2022). The inherent adaptability of hybrid warfare makes it very hard for conventional military forces to counter.

The emergence of digital technologies, particularly artificial intelligence (AI), has significantly influenced both 5GW and hybrid warfare dynamics. With their algorithmic nature, the digital platforms powered by AI facilitate speed in spreading information, enabling actors to shape narratives and sway opinions at an unprecedented speed and scope. For example, social media sites are being run by BOTs for shaping perceptions and rallying support or opposition (Denning, 2001). The ability of real-time communication allows coordinated action among disparate groups, thereby increasing their capacity to conduct hybrid tactics with greater effectiveness. But as these AI-driven 5GW tactics are used to exploit societal sore points like ethnic divisions or political discourse, it is also used to enhance the quality of cyber operations, including the disabling of critical infrastructure or surveillance without direct attack (Barnett, 2004).

The geopolitical implications of 5GW and hybrid warfare go beyond military tactics since they are challenging not only traditional institutions but also societal norms. The blurred lines of distinction between fighters and non-fighters, therefore raise several ethical issues of accountability in war and peace. It is argued by some researchers that the use of hybrid tactics by governments to fight threats from non-state actors or rival countries increases the chances of escalation into traditional warfare (Nadeem et al., 2021).

A synthesis of the current literature on hybrid warfare and cyber threats emanating from AI-driven 5GW to the national security of Pakistan provides a comprehensive analysis of the internal and external dimensions of these threats. However, this research enlists some gaps which need to be filled to have a better understanding of the scale and scope of digital terrorism and its impact on the national security of Pakistan. By addressing these gaps, the literature can add depth to scholarly discussion and will help inform policymakers to navigate the complicated world of cybersecurity in an ever-more interconnected world.

- One of the significant voids in the current literature is the inadequate analysis of the nexus between civil-military relations and the efficacy of cybersecurity measures undertaken by the states (in this case Pakistan) to counter such threats. The majority of studies argue about the military's capture of national security policy, but there is little analysis of how this implementation of cybersecurity initiatives impacts civil governance and norms. This research attempts to analyze specific instances in which coordination between civil and military institutions has an impact on policy effectiveness, particularly in the area of digital security.
- Another key area found lacking in the existing literature is the absence of empirical evidence on civil-military relations for implementing, monitoring and evaluating a cyber-security framework, like Pakistan’s National Cyber Security Policy (NCSP). Further empirical research is required to determine the actual effect of these policies on national security outcomes, pinpointing concrete challenges associated with capacity building, resource allocation, and inter-agency coordination.
- The available literature separates internal and external threats without properly analyzing their interface. Although it is understood that non-state actors such as TTP utilize digital domains for radicalization, there is little that is analyzed on how external cyber actions of states such as India compound such internal vulnerabilities. An integrated analysis of how

external cyber threats by states such as India interface with domestic extremist discourses would provide a more critical understanding of Pakistan's security threats.

- The geopolitical context of Pakistan-India relations is an area of study that needs more comprehensive research. While some studies discuss the threats from outside by adversarial states, they tend not to describe how the dynamics affect domestic cybersecurity policy and social attitudes in Pakistan (Yasin, 2021). The future study should be on how the tensions in the region affect cybersecurity policy and whether the policies are intended to reduce or enhance vulnerabilities.
- There is less focus on the socioeconomic drivers of cybersecurity resilience in Pakistan. The available literature is primarily focused on the technical aspects of cybersecurity, but it underestimates the role of social determinants—education, economic inequality, and public awareness—on the effectiveness of cybersecurity policies (Global Cyber Security Index, 2021). These socio-economic drivers need to be identified to create effective pluralistic plans that take along various segments of society to enhance national security.

DIGITAL TERRORISM: INTERNAL AND EXTERNAL THREATS TO PAKISTAN'S NATIONAL SECURITY

Internal Cyber Threats: Political Disinformation and Digital Radicalization

The internal dynamics of cyber terrorism in Pakistan are a multifaceted threat to national security, particularly since political actors and non-state actors employ cyberspaces for disinformation and radicalization purposes. This research examines how Pashtun Rights Movement (PRM) utilize social media to build their respective narratives that often is construed by scholars like Yasin, M. (2021), and Saeed, A., & Khalid, S. (2020) as threatening the stability of the state. The entity has used a mix of disinformation and twisted facts to make their respective narratives popular by challenging the key institutions of the state, as is detailed in Table 1 and this is seen by Jarvis, L., Macdonald, S., & Nouri, L. (2014) as a threat to the national security of the state.

Table 1: Internal Factors Impacting National Security

Internal Entity	Key Social Media Tactics	Timeline & Major Incidents	Data Sources & Evidence	State Response
Pashtun Rights Movement (PRM)	Ethnic-based mobilization, allegations against the military, advocacy of separatist sentiments	-2018–Present: "#PashtunLivesMatter" trends alleging military's involvement in enforced disappearances - 2023–2024: Online campaigns portraying the state as oppressive	- Interview with Anonymous B, 2025, senior officials on foreign influence in digital narratives - Interview with Anonymous C, 2025, FIA officials on PRM-aligned networks	- Blocking of PRM-affiliated digital platforms - Arrests under sedition & anti-terrorism laws

Case Study: The 2023 #Pashtunrightsmovement Twitter Campaign

The #PashtunRightsMovement emerged in 2023 as a grassroots campaign advocating for accountability regarding enforced disappearances and extrajudicial killings in Pakistan's Pashtun-

majority regions (Table 2). However, state agencies accused it of being a front for "Afghan-sponsored digital terrorism," citing alleged links to hostile actors across the border (*VOA News, Digital terrorism 2024).*

Table 2: Outreach and Impact of #PashtunRightsMovement

Details	Findings	Sources
Tweets/Retweets (6 months)	2.3 million	Twitter Analytics (2023)
Hashtag Reach	15 million users	EU DisinfoLab (2024)
State-Blocked Accounts	1,200 profiles	PTA Report[2] (2023)

Voice of America in its broadcast (2023) aired an interview with an anonymous Pashtun Activist who claimed on air that "We documented 450 cases of missing persons. Instead of answers, we got labelled as 'terrorists.' This isn't justice—it's silencing." However, an Interior Ministry Spokesperson publicly contradicted such claims and categorically told the media at a press briefing (2023); "Foreign actors exploited the movement to destabilize Pakistan. We have evidence of Afghan IP addresses coordinating tweets." Yet, the statement from Amnesty International read, "Linking human rights advocacy to terrorism is a tactic to criminalize dissent" (2023 Report).

From a purely data perspective, the campaign's organic traction (65% of participants were aged 18–35) and forensic analysis by Bellingcat[3] revealed only 12% of accounts showed bot-like behaviour, undermining the "Afghan-sponsored" narrative. Pakistan media outlets, however, amplified claims of financial ties between activists and Kabul-based groups ("National cyber security policy," 2024).

The complexity of the internal spaces of cyber terrorism in Pakistan demonstrates a convoluted nexus of political and non-state groups, which pose significant threats to national security. Political parties such as PTI uses social media for narrative management, whereas rights movements like PRM disseminate politically motivated agendas, which are ethnically driven and anti-establishment in nature. What makes this even more cumbersome for the national security machinery of Pakistan is the intersection of political opposition and radicalization in cyberspace.

The state's reaction to censorship and surveillance poses a risk of encroaching upon civil liberties while, at the same time, failing to touch the source of grievance ("Digital terrorism," 2024). Secondly, the Government's emphasis on narrative control through internet shutdowns or selective action against voices of dissent runs the risk of unwittingly unleashing further unrest. As rights activists suggest, such a policy can alienate the people, who view it as repressive rather than protective ("Rights activists warn," 2024). Such dynamics emphasize the requirement for a more nuanced approach that distinguishes true political debate from genuine risks to national security. Combating such complex threats requires a mature perspective on cyberspace within the larger context of overarching democratic principles to avert undesirable implications.

[2] Annual Report 2023

[3] Bellingcat is a Netherlands-based investigative journalism group that specializes in fact-checking and open-source intelligence (OSINT).

External Cyber Threats: Hostile-State-Sponsored Cyber Operations

The external drivers of cyber terrorism, namely cyber-attacks and propaganda campaigns undertaken by hostile foreign states or transnational non-state actors (NSAs), pose a real concern among the civil and military leadership of Pakistan. Empirical evidence suggests that geopolitical competition between India and Pakistan has now spilled over into cyberspace, where the two countries indulge in cyber activities to destabilize each other. The concept of 5GW particularly applies here, as it refers to a range of activities, which consist of cyber warfare, psychological warfare, and propaganda campaigns (Azad, 2020). India has been accused of using its intelligence agencies, specifically RAW, to carry out subversive activities against Pakistan. Facts attest that India uses Afghan soil to initiate these activities to target places like Balochistan and Khyber Pakhtunkhwa to foster unrest and instability (Hussain & Hussain, 2021; Naazer 2019). The Pakistani establishment has, for example, been concerned with the increasing sophistication of cyber-attacks, which may involve penetrating government databases or disseminating propaganda against state institutions and eroding the trust of citizens (Junejo, S. 2024).

Apart from the threats posed by hostile-foreign-state-sponsored cyber activities, transnational non-state actors (Table 3) also utilize online platforms to disseminate misinformation and radicalize individuals in Pakistan. Tehrik-e-Taliban Pakistan (TTP) and the Baloch Liberation Army (BLA) utilize social media to disseminate extremist ideologies and recruit members. Their capacity to address a global audience through online platforms complicates counterterrorism in Pakistan (Hussain & Hussain, 2021). The convergence of political agendas with extremist narratives makes the dissemination of misinformation common because both end up, advertently or inadvertently, boosting each other's narratives.

This globalized aspect of cyber warfare adds just another layer of challenge to Pakistan's national security and even foreign policy initiatives. Disinformation campaigns not only undermine internal stability but also damage Pakistan's international reputation. For example, efforts by political actors like PTI to manipulate foreign governments' policies using misinformation have strained bilateral relations with major allies like the United States and the United Kingdom (Junejo, S. 2024). Not only do such efforts undermine Pakistan's diplomatic integrity, but they also create a narrative that portrays the country as unstable.

Table 3: Regional Cyber Operations Impacting Pakistan

Actors	Tactics	Frequency	Sources
Indian state actors	Fake news networks	15M users/month reached	EU DisinfoLab (2023)
TTP	Telegram recruitment	1,200 new members (2023)	Pak Institute for Peace Studies (2024)
BLA	Critical infrastructure hacks	4 major incidents (2022–2024)	Dark Web communiqués (2024)

The external characteristics of cyber terrorism in Pakistan reflect a complex interplay of state-led cyber-attacks and transnational non-state actors and present a tremendous threat to national

security. Data in Table 3 reflects that cyberwar dynamics continue to alternate between data breaches, building extremist narratives and running recruitment drives besides using the web-sphere to develop an anti-Pakistan narrative at a global scale.

One of the most significant threats to Pakistan's sovereignty and national security stems from foreign-sponsored cyber intrusions, with India-linked operations being particularly aggressive (Table 4). According to Recorded Future (2024), at least 47 confirmed cyber incidents directly targeted Pakistan's energy grids, financial systems, and diplomatic channels. The Patchwork APT, a sophisticated cyber-espionage group, has repeatedly infiltrated sensitive government institutions, compromising 21 financial systems and 12 energy grids. The ramifications extend beyond mere data breaches—these intrusions have the potential to disrupt economic stability, manipulate financial transactions, and cripple essential services.

Table 4: Internal & External Trends of Cyberattacks Targeting Pakistan (2021–2024)

Variables	Data	Context	Sources
State-sponsored attacks	47 confirmed incidents (India-linked)	Patchwork APT targeted energy grids (12), financial systems (21 incidents), Foreign Office	Recorded Future (2024)
Domestic extremist attacks	68% of social media users exposed to TTP	Radicalization campaigns concentrated in Khyber Pakhtunkhwa and Balochistan	Bytes for Pakistan (2023)
Critical infrastructure breaches	15 major incidents/year	80% involved phishing; 20% ransomware	MOITT (2024)
Disinformation campaigns	750 fake NGOs/media outlets	Indian networks amplified anti-Pakistan narratives to 15M users monthly	EU DisinfoLab (2023)

Convergence of Internal and External Cyber and Hybrid Threats

While external cyber threats pose grave challenges, domestic vulnerabilities are equally concerning. The rise of TTP's online radicalization campaigns has created a digital ecosystem that fosters extremist narratives. According to Bytes for Pakistan (2023), 68% of social media users in conflict-prone areas such as Khyber Pakhtunkhwa and Balochistan have been exposed to TTP-affiliated propaganda. Unlike traditional extremist recruitment strategies, modern radicalization occurs through personalized social media content, exploiting algorithm-driven echo chambers that amplify divisive narratives and erode trust in state institutions. The long-term consequences of this phenomenon are deeply unsettling—a population increasingly susceptible to ideological extremism and insurgent narratives weakens national cohesion and undermines counterterrorism efforts.

The vulnerability of Pakistan's digital infrastructure is further exacerbated by a steady rise in critical breaches. The Ministry of Information Technology and Telecommunications (MOITT, 2024) reported an alarming 15 major cyber incidents annually, with 80 per cent involving phishing attacks and 20 per cent resulting in ransomware disruptions (Table 4). These cyber intrusions, often aimed at state institutions, telecom networks, and financial platforms, highlight the systemic weaknesses in Pakistan's cybersecurity architecture. The reliance on legacy systems, lack of regulatory enforcement, and insufficient cyber literacy among key stakeholders further compound the problem, making national assets highly susceptible to foreign exploitation.

Perhaps the most insidious of all digital threats is the orchestration of large-scale disinformation campaigns aimed at destabilizing Pakistan's political landscape and global standing. Research by EU DisinfoLab (2023) uncovered an extensive network of 750 fake NGOs and media outlets, systematically amplifying anti-Pakistan rhetoric to over 15 million users monthly. These campaigns strategically manipulate social and political fault lines, fabricating narratives that incite sectarian tensions, discredit state institutions, and erode public trust. Disinformation warfare is not just about spreading falsehoods—it is a calculated effort to undermine Pakistan's strategic autonomy, diplomatic credibility, and internal stability.

Case Study: Indian State-Sponsored Phishing Attacks on Pakistan's Foreign Ministry

In 2023, the EU DisinfoLab exposed "Operation KashmirFist," a coordinated phishing campaign by Indian actors targeting Pakistani diplomats. Attackers impersonated EU officials to steal classified documents related to Kashmir policy (Table 5). The EU DisninfoLab[4] revealed that the attacker used spear phishing with malicious .pdf attachments (78%), and fake login portals mimicking EU portals (22%). The attackers managed to have access to the secret documents revealing Pakistan's lobbying strategy to block India's UNSC bid, forcing last-minute revisions.

Table 5: India's 'Operation KashmirFist' exposed by EU Disinfo Lab

Metrics	Findings	Sources
Phishing Emails Sent	1,450	EU DisinfoLab[5] (2023)
Success Rate	23% (334 emails opened)	Anonymous b (2025)
Data Leaked	78 GB (diplomatic cables, meeting transcripts)	EU DisinfoLab (ibid)
Attribution Confidence	94% link to the Indian APT group "Patchwork"	Recorded Future[6] (2024)

[4] EU DisinfoLab develops and maintains an independent European platform on disinformation, providing experts with tools and resources to encourage collaboration.

[5] Indian Chronicles: deep dive into a 15-year operation targeting the EU and UN to serve Indian interests - EU DisinfoLab

[6] Hacktivism: India vs. Pakistan

EU DisinfoLab Analyst revealed that "The attackers used zero-day exploits in Microsoft Exchange servers—a hallmark of state-sponsored actors.". Pakistani Foreign Minister denounced this at the UN ("Pakistani Foreign Minister," 2023) by saying, "This wasn't espionage; it was an act of cyberwar to sabotage our diplomatic efforts." As usual, the Indian External Affairs spokesperson denied this by reverting to an official statement; "Pakistan routinely fabricates cyber threats to deflect from its domestic failures." (Malik, R. 2023).

The confluence of state-sponsored cyber intrusions, extremist propaganda, infrastructure vulnerabilities, and information warfare places Pakistan at the forefront of an evolving security dilemma. The need for a comprehensive national cybersecurity strategy has never been more urgent. This strategy must integrate technological resilience, policy reforms, public awareness campaigns, and regional cyber diplomacy to counter emerging threats effectively.

The battle for national security is no longer fought on conventional frontlines alone—it is waged in the unseen domains of cyberspace, digital narratives, and algorithmic manipulation. Failure to acknowledge and counter these threats would not only endanger Pakistan's strategic interests but also compromise its sovereignty and resilience in the global digital order.

Civil-Military Dynamics in Cybersecurity Governance

The governance of Pakistan's cybersecurity landscape is heavily influenced by civil-military power dynamics, with intelligence agencies playing a dominant role. The Prevention of Electronic Crimes Act (PECA) was initially designed as a counter-cybercrime mechanism, yet, as data **Error! Reference source not found.** depicts, its implementation has disproportionately targeted political dissidents, journalists, and activists, rather than genuine cyber threats ("HRCP. Critical analysis of PECA," 2024). With 1,240 arrests in 2023, where 82% of the detainees were from civil society rather than hostile cyber actors. Since most of these threats are generated from abroad, lack of regional or global mechanisms to nab such perpetrators makes it even worst for states like Pakistan to curb these cyber-crimes.

Table 6: Cyber Security Governance Mechanism in Pakistan

Indicator	Findings	Implications	Source
PECA arrests (2023)	1,240 individuals detained	82% targeted journalists, activists, and opposition figures	HRCP (2024), Abbas, M. (2025), Khattak, A. (2025)
Internet freedom ranking	27/100	Linked to PECA's vague "anti-state activity" clauses	Freedom House[7] (2024)

The National Cyber Security Policy (NCSP, 2021) has further entrenched military dominance, as a majority of the budget allocation goes to the security agencies while civilian agencies such as the Pakistan Telecommunication Authority (PTA) and the Federal Investigation Agency (FIA) remain

[7] Pakistan: Freedom in the World 2024 Country Report | Freedom House

significantly underfunded ("National cyber security policy," 2024). This imbalance has led to a lack of inter-institutional cooperation, creating a fragmented cybersecurity structure that prioritizes state surveillance over comprehensive cyber defence mechanisms. The public perception of cybersecurity governance has also deteriorated. A shift in public sentiment is reflected in Pakistan's internet freedom ranking (Freedom House, 2024). The primary driver of this decline is PECA's vague classification of "anti-state activity," which has been used to suppress critical discourse and opposition narratives rather than mitigate cyber threats from internal and external hostile actors.

Legislative Gaps in Countering Digital Terrorism

Despite the rising threat of digital terrorism, Pakistan's legislative and policy responses remain inadequate and largely misdirected (Table 7). The Prevention of Electronic Crimes Act (PECA, 2016) was originally envisioned to counter cybercriminal activities, but with a conviction rate of just 4% in 2023, HRCP claims that its effectiveness is severely limited. Moreover, 92% of the cases registered under PECA targeted non-violent dissent rather than actual cybercriminal or extremist activities, reflecting an institutional bias that prioritizes political suppression over cybercrime mitigation.

Table 7: Operational Gaps in Countering Digital Terrorism in Pakistan

Policy	Deficiency	Example	Source
PECA (2016)	4% conviction rate (2023)	Used to silence critics: 92% of cases involved non-violent dissent	HRCP (2024)
NCSP (2021)	15% training centres operational	Only 3 of 20 planned centres launched in Punjab/Sindh	NADRA (2024)
Cybercrime Wing efficiency	12,500 websites blocked (2023)	Only 3% had verifiable terror links; 64% targeted political dissent	MOITT (2024)

Similarly, the National Cyber Security Policy (NCSP, 2021) has suffered from poor implementation. While the policy framework included a plan to establish 20 cybersecurity training centres, as of 2024, only three could be operationalized, mostly in Punjab and Sindh (NADRA, 2024). The lack of investment in KP and Balochistan—regions that are particularly vulnerable to digital radicalization and extremist recruitment—indicates a disconnect between cybersecurity policymaking and national security priorities.

Furthermore, the cybercrime wing's enforcement mechanisms have been disproportionately focused on political censorship. Of the 12,500 websites blocked in 2023, only 3% were confirmed to have direct links to terrorist organizations, while 64% targeted political dissenters and independent media outlets (MOITT, 2024). This misallocation of resources weakens Pakistan's ability to combat genuine cyber threats, leaving the state increasingly exposed to hostile digital intrusions.

Socioeconomic Barriers to Cybersecurity Resilience

Pakistan's cybersecurity vulnerabilities are exacerbated by deep-rooted socioeconomic disparities, particularly in rural digital literacy, cybersecurity awareness, and cyber resilience of small enterprises (Table 8). The World Bank (2023) reports that digital literacy in rural Pakistan is only

22%, compared to 58% in urban areas, with Balochistan registering an alarming 11%—highlighting the stark regional divide.

Table 8: Socioeconomic Challenges Hindering Cybersecurity in Pakistan

Factor	Metric	Regional Disparity	Source
Rural digital literacy	22% (vs. 58% urban)	Balochistan: 11%; Punjab: 29%	World Bank[8] (2023)
Cybersecurity awareness	8% understand phishing risks	Khyber Pakhtunkhwa: 5%; Sindh: 12%	Bytes for Pakistan[9] (2023)
Ransomware compliance	71% of SMEs paid ransoms (2023)	Lack of state support; 89% had no cyber insurance	Ransomware. live[10] (2024)

Low cybersecurity awareness further compounds digital vulnerabilities. Only 8% of Pakistanis can correctly identify phishing threats, a figure that drops to 5% in KP and 12% in Sindh (Bytes for Pakistan, 2023). This lack of awareness makes individuals, businesses, and even government institutions susceptible to cyber fraud, data breaches, and digital exploitation.

Additionally, cyber resilience among small and medium enterprises (SMEs) is critically low. A Karachi University study (2024) found that 71% of SMEs targeted by ransomware attacks paid the demanded ransom, with 89% lacking cyber insurance coverage. This high compliance rate encourages further cyber extortion, posing an economic and security risk to the national digital economy.

The analysis underscores the urgent need for a balanced cybersecurity framework—one that prioritizes national security without infringing on democratic freedoms. Addressing civil-military coordination to help address policy gaps, and socioeconomic barriers will be crucial in strengthening Pakistan's cyber resilience in an era of evolving digital threats.

Comparative Analysis and Implications

This study adopts a systematic and multi-layered analytical approach to examining the empirical evidence presented through data tables and case studies. Rather than viewing cyber threats in isolation, it integrates quantitative indicators (e.g., frequency of cyberattacks, scale of disinformation campaigns, institutional response efficiency) and qualitative assessments (e.g., policy effectiveness, geopolitical context, and public sentiment analysis) to construct a comprehensive narrative on Pakistan's cybersecurity vulnerabilities. The methodology follows a comparative lens, assessing both internal cyber threats (e.g., digital radicalization and political disinformation) and external cyber incursions (e.g., state-sponsored espionage and foreign-backed propaganda campaigns).

The tables and empirical evidence presented in this study serve as key instruments in validating theoretical assumptions. For instance, data on cyber breach trends (Table 5), legislative gaps (Table 7), and infrastructure vulnerabilities (Table 4) highlight how institutional weaknesses exacerbate

[8] Digital Progress and Trends Report

[9] cyber_security_strategy_telecom_sector_2023_2028_13-12-2023_1.pdf

[10] Ransomware.live - Victims from Pakistan

cybersecurity threats. By cross-referencing these findings with the independent variables of HWT and CCT, this study establishes a causal relationship between cyber tactics employed by adversaries and the resultant destabilization of Pakistan's national security framework.

Moreover, this research contextualizes its findings within Pakistan's unique geopolitical and governance structures. While HWT explains the confluence of political, cyber, and kinetic strategies used to weaken the state, CCT isolates cyberspace as an independent domain of strategic engagement. The synthesis of these perspectives allows for a more nuanced understanding of digital terrorism, revealing that cyber threats are not merely technical challenges but are deeply intertwined with political instability, governance inefficiencies, and regional power struggles.

Thus, the analytical approach of this study is twofold. Firstly, it provides empirical validation by utilizing data tables and case studies to establish factual linkages between cyber tactics and their impacts on national security. Secondly, it extends theoretical justification by applying HWT and CCT to explain how digital terrorism in the 5GW paradigm translates into real-world governance and security crises.

By adopting this structured analytical framework, the study not only substantiates its arguments but also contributes to the broader discourse on cyber warfare, digital sovereignty, and counter-cyberterrorism strategies in emerging security paradigms.

This comparative analysis critically examines Hybrid Warfare Theory (HWT) and Cyber Conflict Theory (CCT) in the context of Pakistan's cyber vulnerabilities, exploring how these theoretical frameworks illuminate the country's exposure to digital terrorism, hence causing a threat to national security. Given the intricate interplay of internal political narratives, extremist cyber operations, and state-sponsored cyber warfare, Pakistan finds itself at the intersection of hybrid and cyber conflicts**,** making it an ideal case study for understanding the implications of digital terrorism within the broader 5GW framework.

Both theories (HWT and CCT) seek to explain contemporary conflicts where digital, psychological, and conventional tools merge to achieve strategic objectives. However, the key distinction between the two lies in the scope and nature of engagement. HWT provides a multi-domain perspective**,** integrating cyber warfare, psychological operations, and kinetic tactics as part of a broader strategic destabilization campaign. In contrast, CCT isolates cyber operations as an independent domain of warfare, analyzing how actors deploy cyberattacks, espionage, and information warfare to achieve political, military, or economic goals. A comparative breakdown of these two frameworks in Table 9 highlights their distinct yet overlapping dimensions.

Table 9: Comparative Theoretical Framework

Theory	Definition	Core Components	Actors Involved	Primary Strategic Aim
Hybrid Warfare Theory (HWT)	A fusion of conventional, cyber, and irregular tactics to undermine adversaries	Cyberattacks, disinformation campaigns, proxy warfare, and military actions	State actors, insurgent groups, intelligence agencies, political networks	Destabilization of adversaries through multi-domain tactics
Cyber	A conflict model	Digital espionage,	Primarily state	Gaining strategic

Conflict Theory (CCT)	where cyber operations serve as the primary battlefield	malware attacks, network infiltrations, cyber-psychological warfare	actors, but also non-state cyber militias	advantages through cyber superiority

HWT examines the convergence of cyber and kinetic operations**,** CCT underscores how cyberspace itself has become an autonomous theatre of conflict where digital tools alone can destabilize entire states. In Pakistan's case, both frameworks coalesce**,** as cyber terrorism manifests in political disinformation campaigns, state-backed cyber conflicts, and extremist digital mobilization.

Hybrid Warfare and Digital Terrorism in Pakistan: A Converging Threat

Pakistan's national security landscape has been profoundly shaped by hybrid warfare strategies, where adversaries employ cyber-enabled political warfare, insurgency tactics, and disinformation campaigns to weaken state institutions. Unlike traditional conflicts, which rely on direct military engagement**,** hybrid warfare integrates psychological and cyber operations, allowing actors to manipulate narratives and mobilize opposition without deploying physical forces. The following Table 10 outlines some of the key hybrid warfare components observed in Pakistan's cyber domain.

Table 10: Hybrid Warfare in Pakistan

Hybrid Warfare Strategy	**Examples in Pakistan**
Cyber Warfare	PTM's digital campaigns targeting military credibility, particularly after the removal of governments or military operations in troubled areas.
Cyber Propaganda	Indian disinformation networks propagating false narratives about Pakistan's security apparatus
Terrorist Digital Recruitment	TTP's utilization of encrypted social media channels for radicalization and recruitment
State Cyber Espionage	Indian-sponsored hacking attempts against Pakistan's Foreign Office and military institutions

Unlike hybrid warfare observed in conventional military theatres like Ukraine**,** Pakistan's challenges are unique due to the entanglement of internal political struggles with external cyber threats. Domestically**,** political and non-state actor use social media to delegitimize state institutions**,** often amplifying external propaganda narratives. Simultaneously, foreign players leverage digital platforms to manipulate regional stability, making it difficult to distinguish between organic political discourse and deliberate cyber subversion**.**

This dual-layered hybrid threat has led to a reactionary cybersecurity approach in Pakistan, where state responses, such as the Prevention of Electronic Crimes Act (PECA) 2016, focus heavily on narrative control rather than proactive cybersecurity strategies. While these measures suppress dissent, they do little to counteract the technical sophistication of external cyber threats, exposing a critical gap in national cybersecurity policy.

Cyber Conflict and Pakistan's Digital Vulnerabilities

Unlike HWT, which views cyberattacks as a component of broader strategic manoeuvres**,** CCT recognizes cyber operations as an independent domain of war, where states and non-state actors engage in coordinated cyberattacks, espionage, and digital infrastructure sabotage. In Pakistan, cyber conflict manifests in state-sponsored hacking, infrastructure breaches, and coordinated misinformation campaigns, all of which threaten national security and sovereignty. Table 11 illustrates the critical cyber conflict threats faced by Pakistan:

Table 11: Cyber Threats to Pakistan

Cyber Threat	Examples in Pakistan
State-Sponsored Cyber Espionage	Indian intelligence-linked cyberattacks targeting Pakistan's diplomatic communications (e.g., Operation KashmirFist)
Critical Infrastructure Attacks	Ransomware and phishing campaigns targeting Pakistan's financial sector and energy grid
Disinformation Warfare	TTP and ISIS using Telegram and dark web networks to spread radical ideologies
Cyber Surveillance	Alleged foreign-backed digital surveillance targeting Pakistan's military leadership

Pakistan's cyber defenses remain underdeveloped**,** lacking the institutionalized cyber command structures seen in countries like the United States, China, and Russia**.** While PECA 2016 provides a legal framework for digital governance, enforcement remains weak, and Pakistan has no dedicated cyber warfare unit capable of responding to sophisticated cyber threats. The country's reliance on traditional counterterrorism methods further exacerbates these vulnerabilities, as cyber conflicts require specialized digital intelligence operations rather than military responses. This disconnect between conventional security doctrines and cyber threat realities leaves Pakistan highly exposed to both state-sponsored cyber aggression and transnational cybercrime networks.

Interlacing of Hybrid Warfare and Cyber Conflict in Pakistan

The blurring of lines between hybrid warfare and cyber conflict is evident in Pakistan's security challenges, where domestic disinformation campaigns are intertwined with external cyber operations. For instance, following Imran Khan's removal in April 2022, the anti-military sentiment online was amplified by foreign disinformation networks, creating a highly volatile political environment**.** Similarly, Pakistan's ongoing cyber skirmishes with India are not limited to hacking incidents but extend to broader information warfare strategies, where fake news, manipulated narratives, and bot-driven propaganda fuel cross-border hostilities. The convergence of these tactics reinforces Pakistan's hybrid-cyber conflict dilemma, where both internal and external actors simultaneously exploit digital vulnerabilities to achieve their objectives.

CONCLUSION

To effectively counter digital terrorism and cyber threats, Pakistan must adopt a strategic, multi-tiered approach that strengthens technological capabilities, legal frameworks, and international cooperation.

1. Establish a Centralized Cyber Command: Pakistan must create a dedicated National Cyber Command that integrates civilian, military, and intelligence agencies. This entity should

oversee real-time cyber threat analysis, coordinate national responses, and develop long-term cybersecurity policies. Inspired by models such as the U.S. Cyber Command, this body should be equipped with AI-driven threat detection, cyber forensic teams, and rapid incident response units. Pakistan's reaction to cyber terrorism through its policy legislation, military planning, and cybersecurity policies is indicative of a developing conception of national security in the age of the 5GW. Though major efforts have been made through initiatives such as the NCSP and PECA, issues concerning governance, implementation, and civilian rights still need to be addressed adequately enough to silence the national and international bodies monitoring technical and rights-based issues. An interdisciplinary approach that combines effective policy implementation with democratic values is necessary for protecting Pakistan's national interests in a rapidly globalized world. Therefore, this study recommends developing a centralized cyber command by establishing a dedicated military-civilian cybersecurity agency to manage state cyber defences.

2. Strengthen Cyber Education and Public Awareness: A significant gap in Pakistan's cybersecurity infrastructure is the lack of digital literacy and public awareness programs. The state must introduce mandatory cybersecurity education at academic and professional levels, ensuring future generations are equipped to identify and counter digital threats. Additionally, nationwide digital awareness campaigns should educate the public on disinformation, phishing scams, and online radicalization tactics. EU, US and other developing countries like India and Malaysia have introduced fact-checking initiatives by partnering with tech companies to combat fake news. Pakistan could also adopt similar measures to mitigate disinformation while fostering healthy democratic dialogue without curbing civil liberties.
3. Develop Robust Cyber Defense Infrastructure: Pakistan's critical infrastructure—including banking, energy, and defense sectors—remains inadequately protected against cyberattacks. Investing in AI-enhanced cybersecurity tools, blockchain-based digital security, and national threat intelligence sharing networks can enhance resilience against cyber intrusions. With a government cybersecurity budget of just $25 million, Pakistan's resources pale in comparison to India's $500 million allocation, indicating a significant disparity in both funding and strategic focus. The economic impact of cyberattacks in Pakistan is significant, with losses escalating from $80 million in 2020 to $200 million in 2023. In comparison, Bangladesh reported losses of $100 million in 2023, while India experienced damages exceeding $1 billion, largely due to its extensive digital presence and frequent cyber threats from both state and non-state actors (Banerjee, C. 2020). The rising trend of losses related to cyberattacks highlights the pressing need for a resilient cybersecurity framework, upgraded infrastructure and proactive strategies to avert further economic harm.
4. Strengthen International Cyber Diplomacy: Given the cross-border nature of cyber warfare, Pakistan must engage in international cybersecurity alliances and develop bilateral agreements with regional and global partners. Strengthening partnerships with organizations such as INTERPOL, ITU, and CERT can facilitate global intelligence-sharing, capacity-building, and coordinated cyber defense strategies. The strengthening of international cybersecurity alliances can help enrich the vision and scope of the existing infrastructure of cyber security within Pakistan and will help bring in much-needed AI-driven cyber defense mechanisms to counteract foreign cyber espionage.
5. Reform Legal and Policy Frameworks: Current laws, such as PECA 2016, prioritize content regulation over cybersecurity resilience. The government must revise legal frameworks to establish clear cybercrime prevention strategies, penalties for cyber espionage, and protections for digital rights. A well-defined national cybersecurity policy should include provisions for state-level counter-cyberterrorism operations while ensuring transparency

and accountability in digital governance. Instead of an all-encompassing "whole-of-system" and "one-hat-fits-all" approach engaging all government organizations and emphasizing the role of cybersecurity as a fundamental element of national security, regulatory reforms in digital governance need to be adopted to distinguish between dissent and cyberterrorism, ensuring freedom of speech without compromising security.

Pakistan's cybersecurity ranks at 79th (out of 182 assessed countries) globally and 14th in the region[11] underscores the challenges the country faces in establishing a robust security framework. In comparison, regional rivals like India, which holds the 10th position globally and 4th regionally, made significant investments in cybersecurity infrastructure, highlighting the considerable gap in Pakistan's efforts. The digital landscape has become a battleground, placing Pakistan at the forefront of a complex struggle against cyber threats, disinformation, and digital terrorism. By adopting these multi-dimensional strategic policy interventions, Pakistan can strengthen its national security, safeguard digital sovereignty, counter the evolving challenges posed by 5GW, and, in the process, revive civil-military coordination.

References:

Banerjee, C. (2020, June 22). India 6th most targeted by Chinese hackers since 2016. *Times of India.*

Barnett, T. P. M. (2004). *The Pentagon's new map: War and peace in the twenty-first century.* Basic Books.

Buchanan, B. (2020). *The hacker and the state: Cyber-attacks and the new normal of geopolitics.* Harvard University Press.

Bytes for Pakistan. (2023). Digital disinformation in Pakistan: Trends and countermeasures. *Bytes for Pakistan.* cyber_security_strategy_telecom_sector_2023_2028_13-12-2023_1.pdf.

Clarke, R. A., & Knake, R. K. (2010). *Cyberwar: The next threat to national security and what to do about it.* HarperCollins.

Denning, D. E. (2001). *Cyberterrorism: The next wave?* United States Institute of Peace Press.

Digital terrorism and political dissent in Pakistan. (2024, August 27). *VOA News.*

EU DisinfoLab. (2023). *Operation KashmirFist: Cyber espionage and disinformation.* https://www.disinfo.eu/publications/operation-kashmirfist-cyber-espionage-and-disinformation/

Fact-checking in the digital era: Lessons for Pakistan. (2023). *Economic Times.*

Global Cyber Security Index. (2021.) International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCSI2021.aspx; Global Cyber Security Index (2021).

Hoffman, F. G. (2017). Hybrid warfare and future conflicts. *Strategic Studies Quarterly, 11*(4), 34-45.

Human Rights Commission of Pakistan (HRCP). (2024, Feb. 15). Critical analysis of PECA's implementation: Disproportionate targeting of political dissidents, journalists, and activists [Press release]. *HRCP.*

Hussain, S., & Hussain, M. (2021). Cybersecurity challenges in Pakistan: A geopolitical perspective. *Journal of Cyber Policy, 6*(2), 115-30.

[11] Global Cybersecurity Index 2020

Jarvis, L., Macdonald, S., & Nouri, L. (2014). Cyberterrorism: Understanding the concept through a broader lens. *International Journal of Cyber Warfare and Terrorism, 4*(1), 45-60.

Junejo, S. (2024, July 25). Threats of digital terrorism for Pakistan. *Daily Times.*

Kello, L. (2017). *The virtual battlefield: Cyber power in global politics.* Georgetown University Press.

Krishnan, A. (2022b). Fifth-generation warfare, hybrid warfare, and grey zone conflict. *Journal of Strategic Security, 15*(3), 78-95.

Malik, R. (2023, April 30). Cyber espionage a big threat. *Pakistan Today.*

Mumford, A. (2013). *Proxy warfare.* Polity Press.

Naazer, M. A. (2019). Internal conflicts and opportunistic intervention by neighbouring states: A study of India's involvement in insurgencies in South Asia. *IPRI Journal, 18*(1), 63-100.

Nadeem, M. A., Mustafa, G., & Kakar, A. (2021). Fifth generation warfare and its challenges to Pakistan. *Pakistan Journal of International Affairs, 35*(2), 101-20.

NADRA. (2024). *Cybersecurity performance report 2024.* NADRA.

National cyber security policy (NCSP, 2021) deepens military dominance at the expense of civilian agencies. (2024, February 15). *Dawn*.

Nisar, M. (2020). 5GW and hybrid warfare: Its implications and response options. *Journal of Security Studies, 8*(1), 33-50.

Pakistani Foreign Minister. (2023, Mar. 15). Statement at the United Nations: "This wasn't espionage; it was an act of cyberwar to sabotage our diplomatic efforts." [Speech transcript]. *United Nations.*

Rattray, G., & Healey, J. (2011). Cyber deterrence and cyber war. *RAND Corporation.*

Recorded Future. (2024). *Pakistan cyberattack trends 2021–2024.* Author.

Rights activists warn policy may alienate public. (2024, March 10). *Dawn*.

Saeed, A., & Khalid, S. (2020). Digital terrorism in Pakistan: An emerging threat landscape. *Pakistan Journal of Criminology, 12*(1), 55-70.

Yasin, M. (2021). Cybersecurity policies in South Asia: Regional challenges and solutions. *Journal of Cyber Studies, 9*(2), 150-65.

World Bank. (2023). World Development Report 2023: Cybersecurity and development. *Author*.

Date of Publication	September 15, 2024