Conceptualizing Digital Terrorism in Pakistan and Its Solution in the Light of Shariah

Mr. Muhammad Abdullah Ghazi
PhD Scholar, NUML Islamabad
Email: abdullahghazindu@gmail.com

Abstract
Digital terrorism is the use of digital technologies and the internet by different terrorist organizations to carry out, advocate, or support violent activities and chaos caused due to their ideological or political objectives. The paper aims to explain the new concept of digital terrorism by analysing its different meaning and definitions. It also scrutinises the impact of digital terrorism on the peace and security of the country as it becomes a significant threat in Pakistan. The paper aims to explore the multifaceted nature of digital terrorism, focusing on social media propaganda, sectarianism, anti-state and anti-army sentiments, and the resulting insecurity and insurgency. The study will also investigate that how these elements contribute to the destabilization of the country and propose strategies to counteract these threats. Furthermore, the research also analyse solution in the light of shariah. The paper underlines the pressing need for a robust framework to comprehend digital terrorism and formulate effective strategies and policies as countermeasures. With the continuous evolution of cyber threats, it is imperative for governments and organizations to formulate the strategies effectively to counter this emerging threat.
Keywords: Digital terrorism, Cyber Security, Cyber Terrorism, Social Media

Introduction

Globalization has significantly enhanced the technology sector, particularly in the realm of information and communication technologies. While globalization has contributed significantly to global prosperity, it is also true that terrorism has appeared as a great threat to international peace and security. There is an ongoing debate about whether terrorism has increased as a direct consequence of globalization or if it is primarily the result of certain communities being excluded from the benefits of globalization, which has transformed them into a global threat. As a result, the terrorism has emerged as a major threat than ever such as digital terrorism.[1] Digital terrorism involves the use of the internet, digital platforms, and communication technologies to carry out terrorist activities or advance terrorist agendas. Such activities can include spreading propaganda, stealing or manipulating data, disrupting vital infrastructure systems, spreading extremism etc. In contrast to traditional forms of

terrorism that rely on physical violence, digital terrorism harnesses the anonymity and extensive reach of the internet to attain political, ideological, or religious aims without being confined by geographic limitations. Digital terrorism can take the form of hacking into government systems, sabotaging critical infrastructure, attaining confidential data, and leveraging social media platforms to influence people. Theohary and Rollins defines digital terrorism as an unauthorized attacks and threats aimed to hack computers, networks, and the data they store and transmit.[2] Digital terrorism is therefore, the intentional use of methods and tools, typically by non-state actors and terrorist organisations to spread fear, distress and panic by disrupting population and government organisations thus possess great threat to peace and security of a country. A more comprehensive definition of digital terrorism is "Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[3] According to Denning; "Cyber-terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as Cyber-terrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of Cyber-terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[4]

In Pakistan, digital terrorism has become a substantial threat because of the country's persistent security challenges and the growing prevalence of technological advancements. Terrorist groups and organizations have leveraged these technologies to radicalize young people, manage their activities, and disseminate extremist narratives. The digitalisation in Pakistan, characterized by increased use of social media and connectivity, has opened opportunities for both state and non-state actors to participate in cyber warfare and manipulate information. The changing landscape of digital terrorism necessitates a comprehensive approach that includes improved cybersecurity measures, legislative initiatives, and international cooperation to effectively address this contemporary threat.5 This phenomenon includes various activities, such as cyber-attacks on government and private sector, the dissemination of radical content online, and the utilization of social media platforms for

propaganda purposes. Security challenges in Pakistan is characterized by persistent challenges from a range of extremist groups and militant organisations. These actors have adjusted to the digital era by utilizing technology to circumvent conventional security measures and engage broader audiences. The utilization of encrypted communication means and channels, various social media platforms, and dark web forums has given space to these groups to manage their activities, radicalize susceptible individuals, and spread fear without the limitations of physical borders.6 The rapid expansion of internet access and its use as well as advance mobile technology in Pakistan has facilitated this transition. Although, digital connectivity provides many economic and social benefits, it also opens the door to potential threats to security of a country. The effects of digital terrorism in Pakistan go beyond the immediate security threats as it erodes public trust, destabilizes socio-political conditions, and poses significant risks and challenges to national security and economic development of the country. Addressing digital terrorism necessitates a strong and comprehensive strategy and framework that involves enhancing cybersecurity procedures, implementing legislative reforms, raising public awareness, and promoting international collaboration to tackle the global aspects of the threat. The main objectives of the research are to analyse the role of social media in propagating digital terrorism in Pakistan; to examine the anti-state propaganda on national security, different methods used by terrorist organizations to recruit and radicalize individuals online. The research will also propose effective countermeasures to mitigate the influence of digital terrorism.

Literature Review

Digital terrorism involves utilizing digital technologies to enable, promote, or carry out acts of violence and coercion driven by ideological or political motives. As information technology advances rapidly and internet usage becomes more widespread, terrorist organizations have increasingly utilized digital platforms for recruitment, radicalization, and the execution of their agendas. This literature review explores the main themes and findings from current research on digital terrorism, emphasizing its definitions, different means/methods, consequences, and the changing phenomena of cyber threats.

According to Gabriel Weimann Digital terrorism signifies the transformation of traditional terrorist tactics into the online sphere, where anonymity and global accessibility enhance the capacity of extremist groups to influence and disrupt.[7] The term originated from the intersection of cyber operations and terrorism, highlighting how the digital era has reshaped the nature of threats confronting nation-states and societies.

Furthermore, Sara Zeiger and Joseph Gyte's research underscores how terrorist groups exploit a range of digital tools to advance their goals. Platforms such as Facebook, Twitter, and Telegram, along with encrypted messaging services, offer an optimal space for disseminating propaganda, recruiting members, and organizing operations. Digital terrorism has emerged as a major concern in Pakistan, driven by the activities of both domestic and transnational terrorist organizations.[8] Digital terrorism signifies the transformation of traditional terrorist tactics into the online sphere, where anonymity and global accessibility enhance the capacity of extremist groups to influence and disrupt. The proliferation of extremist content online has fostered an environment in which radical ideologies can be nurtured without direct interaction, posing significant challenges for counterterrorism initiatives.[9] Scholars like Saba and Areesha emphasizes that the extensive implications of digital terrorism for national security are significant. Cyber-attacks aimed at government databases, critical infrastructure, and private sector assets can lead to economic harm and undermine public trust. Pakistan has encountered instances of such disruptions, highlighting the necessity of cybersecurity as a vital element of national defense.[10] Research indicates that terrorist organizations exploit digital channels to radicalize individuals, particularly youth. Groups like ISIS, Tehrik-e-Taliban Pakistan (TTP), and Baloch Liberation Army (BLA) have effectively utilized social media for recruitment and propaganda dissemination. Studies highlight that these organizations often target specific demographics, including women, to spread their ideologies and gain support. Literature on countering digital terrorism points to several approaches, including enhanced cybersecurity protocols, international cooperation, and legislative measures. The Pakistani government has recognized the need to combat digital terrorism through various measures. Initiatives such as the "Azm-e-Istehkam" operation aim to address both traditional militancy and the new challenges posed by digital platforms. However, there are concerns that the government's approach may also target political dissent under the guise of combating digital terrorism, raising issues related to freedom of speech and civil liberties.[11]

The existing legal framework in Pakistan regarding cybercrime is seen as insufficient. While laws like the Prevention of Electronic Crimes Act (PECA) 2016 address some aspects of cybercrime, there is a lack of clarity regarding definitions and enforcement mechanisms specifically related to digital terrorism. Scholars argue for the need for more robust legislation that can effectively address the complexities of cyber threats while protecting individual rights.[12] General Asim Munir, the Chief of Army Staff, has characterized digital terrorism as a significant threat to

national security. He emphasizes that digital platforms are being exploited to disseminate misinformation and incite unrest against state institutions. He also warns that such activities aim to create discord between the military and the public, indicating a need for a robust response to what he describes as "digital terrorism".[13] Nawal Munir Ahmad discusses the evolution of internet governance in Pakistan, emphasizing the need for robust governance mechanisms to address both cybercrime and digital terrorism effectively. She advocates for policies that enhance cybersecurity while promoting digital literacy among citizens.[14] Her work suggests that improving public awareness and engagement with internet governance can help mitigate risks associated with digital terrorism.

The perspectives of these scholars illustrate a complex landscape regarding digital terrorism in Pakistan, encompassing military concerns about national security, civil rights advocacy against suppression of dissent, and calls for improved cybersecurity measures. The ongoing debate highlights the need for a nuanced approach that balances security in an increasingly digitized world. Despite substantial research, there remain gaps in understanding the full scope of digital terrorism's socio-political impact and the effectiveness of countermeasures in developing regions like Pakistan. Limited empirical studies on the psychological effects of online radicalization and the long-term outcomes of digital counterterrorism policies are areas that warrant further exploration. In Pakistan, addressing digital terrorism requires a blend of legislative action, technological investment, public awareness, and international cooperation to mitigate the threat and protect national security.

Nature and Forms of Digital Terrorism

Digital terrorism in Pakistan involves the adaptation of conventional terrorist tactics to the digital sphere. This includes utilizing online platforms for recruitment, radicalization, and the dissemination of misinformation, creating substantial threats to national security.[15] The military's anti-terror operation, "Azm-e-Istehkam," highlights the evolving nature of threats by targeting both traditional militancy and the growing impact of digital terrorism.[16] General Asim Munir has expressed concerns over the misuse of social media to spread false narratives and provoke unrest against state institutions, describing these actions as a form of digital terrorism aimed at fostering division between the military and the public.

- ### Cyber-Attacks and Hacking Incidents in Pakistan

In recent years, Pakistan has experienced a significant rise in cyber-attacks and hacking incidents, highlighting an increasing threat to national security. According to Kaspersky, the number of overall cyber threats in

Pakistan rose by 17% in 2023, with the company blocking 16 million cyber attacks during that year alone. Notably, attacks involving banking malware surged by 59%, while ransomware incidents increased by 24%.[17] Moreover, spyware attacks experienced a staggering 300% increase in early 2024 compared to the previous year, highlighting a dramatic escalation in data infiltration and espionage activities.[18] These attacks have primarily targeted critical sectors, including government, finance, and other key institutions, raising significant concerns about the growing sophistication and intensity of cyber threats in Pakistan.[19] The military's emphasis on addressing "digital terrorism," as articulated by Chief of Army Staff General Asim Munir, indicates a shifting strategy in tackling both conventional and digital threats. This encompasses worries about misinformation disseminated via social media, viewed to provoke unrest against state institutions. Additionally, reports of internet slowdowns and heightened surveillance exacerbate the situation, raising concerns about possible violations of civil liberties in the context of attempts to manage the narrative related to national security matters. These developments highlight the pressing need for improved cybersecurity measures and a comprehensive strategy to effectively tackle the complex nature of cyber threats facing Pakistan.

- **Use of social media for recruitment and propaganda**

The use of social media for recruitment and propaganda in Pakistan has become a critical concern, as various extremist groups exploit these platforms to disseminate their ideologies and attract new members. Research indicates that organizations such as the Tehrik-e-Taliban Pakistan (TTP), the Baloch Liberation Army (BLA), and ISIS utilize social media channels like Facebook, Twitter, and Telegram to target vulnerable youth. These groups employ a range of strategies, including the dissemination of propaganda that glorifies violence and frames their actions as part of a legitimate struggle for rights or religious obligations.For instance, the TTP effectively uses social media to share videos and written statements that promote its ideology and justify its attacks as acts of jihad. Their content often resonates with disillusioned young people seeking purpose, making them susceptible to radicalization. Similarly, the BLA leverages social media to project itself as a freedom-fighting organization, focusing on issues like alleged human rights abuses by the Pakistani government. By portraying their struggle in a heroic light, they aim to recruit individuals who feel marginalized. Moreover, the military's response to this phenomenon has included launching operations like "Azm-e-Istehkam," which aims to counter both traditional militancy and the digital threats posed by extremist propaganda. However, this has raised concerns about potential overreach and censorship, as rights activists warn that vague

definitions of "digital terrorism" could be used to suppress dissenting voices online. Overall, the interplay between social media and radicalization in Pakistan highlights the urgent need for effective countermeasures that balance national security with the protection of civil liberties.

Factors Contributing to Digital Terrorism

The drivers of digital terrorism in Pakistan are complex and intricately tied to the country's socio-economic and political context.

- **Socio-Economic Vulnerabilities**

  High levels of unemployment, poverty, and inadequate access to education among the youth provide a conducive environment for radicalization. The United Nations Development Programme (UNDP) emphasizes that these socio-economic challenges leave young individuals vulnerable to extremist ideologies, as they often turn to groups offering a sense of purpose and solutions to their frustrations.[20]

- **Exploitation of Social Media**

Terrorist organizations such as Tehrik-e-Taliban Pakistan (TTP), Baloch Liberation Army (BLA), and ISIS effectively utilize social media platforms like Facebook and Twitter to disseminate extremist propaganda, recruit new members, and plan attacks. These platforms offer a means to engage with vulnerable youth, exploiting their feelings of isolation or frustration. The accessibility of these digital spaces facilitates the rapid spread of radical ideas without requiring direct contact, making it easier for extremists to influence and enlist potential followers.[21] By leveraging emotional appeals and creating echo chambers, these groups can reinforce their narratives and attract individuals who may feel marginalized or disillusioned with their circumstances.

- **Lack of Awareness and Countermeasures**

There is a significant lack of structured awareness initiatives by the government or educational institutions concerning the dangers of online radicalization. This gap enables terrorist groups to function with relative freedom, worsening the problem.

- **Political Instability and Misinformation**

Pakistan's political climate, marked by instability and a lack of trust in state institutions, has contributed to the growing use of digital platforms for political dissent. The military's emphasis on combating "digital terrorism" has sparked concerns over potential censorship and surveillance, which could suppress legitimate political discussions while not effectively addressing the underlying causes of radicalization.[22]

- **Technological Expertise Among Extremists**

Many individuals engaged in extremist activities have acquired technological skills that enable them to effectively navigate online platforms. This expertise allows them to create tailored messages that appeal to particular audiences, thereby strengthening their recruitment efforts.[23]

- **Geopolitical Tensions**

Regional geopolitical dynamics also contribute to creating an environment that facilitates digital terrorism. External influences and conflicts can intensify internal divisions, prompting groups to use digital platforms for recruitment and propaganda as part of larger ideological struggles.[24]

Impacts on National Security

The impact of digital terrorism on Pakistan's national security is significant and multifaceted, reflecting both immediate threats and long-term challenges such as Increased Cyber Threats, Geopolitical Vulnerabilities, Espionage and Data Breaches, Military Response and Surveillance, Hybrid Warfare Concerns etc.

- **Threats to government and private sector systems**

Digital terrorism poses a significant and multifaceted threat to both government and private sector systems in Pakistan, impacting national security, economic stability, and public trust. In recent years, the country has witnessed a dramatic increase in cyber threats, with Kaspersky reporting a 17% rise in overall cyber incidents in 2023, resulting in the blocking of 16 million attacks. Among these, banking malware attacks surged by 59%, ransomware incidents increased by 24%, and spyware attacks rose by 36%.[25] These alarming statistics highlight the vulnerability of critical sectors such as finance, telecommunications, and e-commerce to cybercriminal activities. Government institutions are particularly at risk, as they often hold sensitive information that can be exploited for espionage or sold on the dark web. Such breaches not only compromise national security but also erode public trust in governmental capabilities to protect citizens' data.The economic repercussions of digital terrorism are profound. Cyber incidents can lead to substantial financial losses for both public and private entities due to recovery costs, reputational damage, and potential regulatory penalties. As businesses increasingly digitize their operations, the fear of cyberattacks can deter investment and disrupt market stability.[26] The lack of a robust cybersecurity infrastructure further exacerbates these issues. Despite improvements in Pakistan's Global Cybersecurity Index ranking, many institutions still struggle with inadequate resources and insufficient investment in protective measures. A significant gap exists in skilled

personnel capable of implementing comprehensive cybersecurity strategies, leaving critical systems exposed to evolving threats. Moreover, the rapid advancement of technologies such as artificial intelligence adds another layer of complexity to the threat landscape. Cybercriminals are increasingly adopting sophisticated methods, including automated attacks powered by AI, making it more challenging for organizations to defend against these evolving tactics. Geopolitical tensions also play a crucial role in exacerbating cyber threats. State-sponsored actors or hostile entities may target Pakistan's digital infrastructure as part of broader strategic objectives, further complicating the security environment. In response to these challenges, there is an urgent need for a comprehensive national cybersecurity strategy that encompasses both government and private sector collaboration. This strategy should focus on enhancing cybersecurity measures, fostering public awareness about digital threats, and investing in the development of skilled personnel equipped to combat cybercrime effectively. By addressing these vulnerabilities and strengthening defenses against digital terrorism, Pakistan can better safeguard its critical infrastructure and maintain economic stability while protecting the privacy and security of its citizens.

- **Influence on public safety and social cohesion**

The influence of digital terrorism on public safety and social cohesion in Pakistan is profound and far-reaching. Digital terrorism exploits online platforms to spread fear, disrupt social harmony, and challenge state authority, which can significantly undermine public safety and national security. Terrorist organizations utilize digital spaces to propagate extremist ideologies, recruit new members, and coordinate violent activities. The ease of access to these platforms enables them to reach a large audience, including vulnerable individuals, often resulting in radicalization and violent actions. Social cohesion is also severely affected as digital terrorism can fuel divisions within society by amplifying sectarian, ethnic, and political tensions. The use of social media to disseminate hateful and inflammatory content increases polarization, creating mistrust and hostility among different social groups.[27] In Pakistan, this digital divide is exacerbated by the political instability, economic inequality, and social vulnerabilities present in the country.

- **Economic consequences**

Digital terrorism has profound economic consequences for Pakistan, affecting various sectors and hindering overall growth. The increasing frequency and sophistication of cyber-attacks have led to significant financial losses, diminished investor confidence, and

disruptions in normal business operations. According to Kaspersky, the number of cyber threats in Pakistan rose by 17% in 2023, with 16 million cyber attacks blocked during the year. Notably, attacks using banking malware surged by 59%, while ransomware incidents increased by 24%. These statistics highlight the vulnerability of critical sectors such as finance and telecommunications to cyber threats, which can deter foreign direct investment (FDI) and domestic investment. The impact of terrorism on economic growth has been well-documented. Research indicates that a one percent increase in terrorism can reduce FDI by 0.104 percent and domestic investment by 0.039 percent. This decline in investment directly correlates with lower economic growth rates, as evidenced by the drop in capital formation from 17.46% of GDP in 2005 to 13.51% in 2015 due to terrorism-related activities. The cumulative cost of terrorism to Pakistan's economy since the events of September 11, 2001, is estimated at around $126.79 billion, equivalent to approximately Rs. 10,762 billion, illustrating the long-term economic repercussions of sustained instability. Moreover, the rising costs associated with cybersecurity breaches—such as recovery expenses, reputational damage, and regulatory penalties—further exacerbate the economic strain on businesses. As organizations increasingly digitize their operations, the threat of cyber incidents can destabilize markets and hinder growth in critical sectors like e-commerce and digital finance. The lack of robust cybersecurity infrastructure also poses a significant challenge; many institutions are ill-equipped to handle the escalating threat landscape due to insufficient funding and a shortage of skilled personnel. In addition to direct financial impacts, digital terrorism can disrupt normal economic activities, leading to increased costs of doing business and loss of market share in international trade. The adverse effects on tax collection and exports due to terrorism-related disruptions further complicate Pakistan's economic recovery efforts.

Government and Security Responses

The government and security responses against digital terrorism in Pakistan have evolved significantly in recent years, driven by the increasing frequency and sophistication of cyber threats. Recognizing the urgent need to bolster its cybersecurity infrastructure, Pakistan has initiated several key measures aimed at enhancing national security and protecting critical digital assets. One of the most significant developments is the establishment of a National Cybersecurity Authority, which is set to be operational by next year. This authority will oversee cybersecurity efforts, tighten surveillance, and protect against data breaches and cyber attacks targeting national institutions.[28] The National Cyber Emergency Response Team (CERT) is being upgraded to fulfil this role, with plans to establish a lab that ensures

organizations deploy robust security hardware and software. This initiative responds to recent incidents where key institutions, including banks and state-owned enterprises, suffered data breaches, often attributed to foreign cyber attackers, particularly from India. In addition to establishing a dedicated cybersecurity authority, Pakistan has implemented the National Cyber Security Policy, introduced in 2021.[29] This comprehensive framework outlines strategies for enhancing cybersecurity across various sectors, emphasizing the importance of governance, capacity building, and public awareness. The policy includes 17 distinct deliverables aimed at addressing critical cyber issues that threaten national security. A Cyber Governance Policy Committee (CGPC) was also formed to oversee the implementation of this policy and ensure coordination among various stakeholders. Moreover, the Prevention of Electronic Crimes Act (PECA) enacted in 2016[30] provides a legal framework for addressing cybercrime, including provisions for preventing unauthorized access and prosecuting cyber offenders. The recent amendment bill aims to strengthen these laws further by establishing a Digital Rights Protection Authority to oversee social media platforms and enforce regulations related to online conduct. The Pakistan Telecommunication Authority (PTA) has also launched the Cyber Security Strategy 2023-2028 for the telecom sector, which aligns with the National Cyber Security Policy.[31] This strategy focuses on training personnel in cybersecurity practices and ensuring compliance with regulatory frameworks. Despite these advancements, challenges remain. Pakistan still ranks low on the Global Cyber Security Index, indicating a need for improved technical and organizational measures. The country faces significant hurdles in terms of inadequate funding for cybersecurity initiatives and a shortage of skilled professionals in the field. Additionally, public awareness about cybersecurity risks needs enhancement to foster a culture of vigilance among citizens. While Pakistan has made substantial strides in addressing digital terrorism through policy frameworks and institutional reforms, ongoing efforts are essential to build a resilient cybersecurity posture capable of mitigating emerging threats and safeguarding national interests in an increasingly digital world.

Challenges in Countering Digital Terrorism in Pakistan

Countering digital terrorism in Pakistan presents numerous challenges that complicate efforts to enhance national security and protect critical infrastructure. One of the foremost challenges is the insufficient cybersecurity infrastructure. Despite recent improvements in the Global Cybersecurity Index, Pakistan still lags in technical and organizational measures necessary to combat cyber threats effectively. Many institutions lack adequate funding and resources to implement comprehensive

cybersecurity strategies, which leaves them vulnerable to attacks. The reliance on outdated technologies and insufficient investment in modern cybersecurity solutions exacerbate these vulnerabilities, making it difficult to respond to evolving threats. Another significant challenge is the shortage of skilled cybersecurity professionals. The rapid growth of digital technologies has outpaced the development of local expertise in cybersecurity, forcing many organizations to depend on foreign solutions. This dependence not only highlights the lack of domestic capabilities but also exposes Pakistan to external pressures and potential geopolitical influences.[32] The limited pool of trained personnel hampers the ability to develop and implement effective cybersecurity measures, thereby increasing susceptibility to cyberattacks. Moreover, geopolitical tensions play a critical role in shaping the cybersecurity landscape. Pakistan faces persistent threats from state-sponsored cyber activities, particularly from neighbouring countries like India, which has been enhancing its cyber warfare capabilities. These geopolitical dynamics create an environment where cyber threats are not just criminal activities but also tools of statecraft, complicating the security response. The complexity of cyber threats further complicates counter-terrorism efforts. Cybercrime encompasses a wide range of activities, including hacking, identity theft, financial fraud, and espionage targeting critical infrastructure. This diversity requires a multifaceted approach that includes not only technical solutions but also legal frameworks and public awareness initiatives. However, the current legal framework for addressing cybercrime is often inadequate and poorly enforced, making it challenging to prosecute offenders effectively. Additionally, there is a pressing need for public awareness and education regarding cybersecurity risks. Many users remain unaware of best practices for online safety, making them easy targets for cybercriminals. Without widespread education campaigns to inform citizens about potential threats and protective measures, efforts to combat digital terrorism may be undermined. Lastly, the lack of a cohesive national strategy for cybersecurity poses a significant hurdle. While initiatives such as the National Cybersecurity Policy have been introduced, effective implementation remains a challenge due to bureaucratic inefficiencies and lack of coordination among various government agencies.[33] A unified national approach is essential for creating an integrated defense mechanism capable of addressing the multifaceted nature of digital terrorism. In summary, countering digital terrorism in Pakistan requires addressing these challenges through comprehensive investment in cybersecurity infrastructure, developing local expertise, enhancing legal frameworks, fostering public awareness, and establishing a cohesive national strategy.

By tackling these issues head-on, Pakistan can better safeguard its digital landscape and enhance its resilience against emerging cyber threats.

Role of International Collaboration

International collaboration plays a vital role in mitigating digital terrorism in Pakistan, addressing the complex and evolving nature of cyber threats that transcend national borders. As the digital landscape expands, extremist groups increasingly exploit technology for recruitment, propaganda, and operational planning, necessitating a coordinated global response. One significant initiative is the partnership between Pakistan and the United Nations Office on Drugs and Crime (UNODC), which aims to enhance the country's capacity to handle electronic evidence in terrorism-related cases.[34] In January 2022, this collaboration resulted in the launch of a "Customized Practical Guide for Pakistan on Requesting Electronic Evidence Across Borders." This guide equips law enforcement and judicial officials with essential tools to effectively gather and utilize electronic evidence, thereby improving the prosecution of terrorism cases. The emphasis on international cooperation reflects Pakistan's recognition that combating digital terrorism requires not only domestic efforts but also collaboration with global partners to strengthen legal frameworks and enhance investigative capabilities.[35] Additionally, Pakistan has actively participated in various international forums focused on cybersecurity and counter-terrorism. The country is involved in discussions under the United Nations framework, including the Counter-Terrorism Committee, which encourages member states to cooperate in preventing terrorists from exploiting technology. These discussions emphasize the importance of sharing intelligence, best practices, and resources to counteract the digital tactics employed by extremist groups. Moreover, Pakistan's engagement with regional organizations like the Shanghai Cooperation Organization (SCO) and the ASEAN Regional Forum (ARF) facilitates dialogue on cybersecurity challenges faced by member states. These platforms provide opportunities for information sharing and collaborative strategies to combat cyber threats that affect regional stability. The need for public-private partnerships is also highlighted as a crucial component of effective counter-terrorism efforts. By involving technology companies and civil society organizations, Pakistan can leverage their expertise in developing counter-narratives and technological solutions to combat online radicalization. Such collaborations can enhance resilience against digital terrorism by fostering a more secure online environment. Despite these initiatives, challenges remain. The rapid evolution of cyber threats necessitates continuous adaptation and improvement of strategies. Pakistan must invest in building local cybersecurity capabilities while also seeking technical assistance from

more advanced nations. This includes developing training programs for law enforcement personnel and enhancing public awareness about cybersecurity risks. In conclusion, international collaboration is essential for Pakistan to effectively mitigate digital terrorism. By strengthening partnerships with global organizations, engaging in regional dialogues, and fostering public-private cooperation, Pakistan can enhance its capacity to combat cyber threats while ensuring that its strategies are aligned with international standards and best practices. This multifaceted approach will not only protect national security but also contribute to global efforts against digital terrorism.

Digital Terrorism in the Light of Shariah

Digital terrorism represents a contemporary challenge in today's digital landscape, threatening security, ethical standards, and social cohesion. To effectively tackle this issue within the framework of Shariah, it is essential to adopt a holistic strategy that emphasizes justice, accountability, and the encouragement of ethical conduct.[36] Shariah underscores the importance of preventing harm to others (darar) and safeguarding life, property, and dignity. Potential solutions involve promoting awareness of the ethical use of technology, implementing stringent regulations on digital platforms to prevent abuse, and ensuring that offenders are held accountable through just legal systems. Furthermore, Shariah advocates for cooperation among individuals, communities, and governments to maintain peace and security, while also emphasizing the importance of education in combating extremist ideologies. Additionally, Shariah promotes collaboration among individuals, communities, and governments to preserve peace and security, while highlighting the critical role of education in countering extremist ideologies.

In the fight against digital terrorism, Shariah highlights the concepts of collective responsibility (mas'ooliyyah) and the safeguarding of societal welfare (maslahah). Islam encourages proactive strategies, including educating individuals on the ethical use of technology and promoting a culture of accountability in online environments. Governments and organizations are urged to establish advanced monitoring systems to identify and prevent cybercrimes while maintaining transparency and fairness. Shariah also emphasizes the importance of dialogue and deradicalization programs to tackle the underlying causes of extremism and digital violence. By fostering values of peace, mutual respect, and lawful behavior, Shariah offers a framework for establishing a secure and harmonious digital environment that aligns with the broader objectives of justice and the safeguarding of humanity.

Shariah underscores the importance of fostering peace, mutual respect, and compliance with lawful principles, offering a comprehensive framework to tackle contemporary issues like digital terrorism. By promoting ethical behavior and condemning actions that cause harm to individuals or communities, it provides clear guidance for building a safe, balanced, and harmonious digital landscape. Shariah's principles emphasize justice, accountability, and the preservation of human dignity, ensuring that technology is utilized to advance welfare and prevent harm. This holistic approach aligns with Shariah's broader objectives of protecting life, property, and societal harmony across all aspects of life, including the digital sphere.

Surah Al-Ma'idah emphasizes themes of justice, societal welfare, and the consequences of harmful actions, providing valuable guidance that can be applied to addressing digital terrorism. Verses like 5:8 ("Be steadfast in justice...") stress the significance of fairness, while others caution against spreading corruption and causing harm—principles that are particularly pertinent to combating the misuse of digital platforms. **Verse 33 of Surah Al-Ma'idah** "Indeed, the penalty for those who wage war against Allah and His Messenger and strive upon earth [to cause] corruption is none but that they be killed or crucified or that their hands and feet be cut off from opposite sides or that they be exiled from the land." This verse addresses those who spread corruption, akin to digital terrorism that jeopardizes societal peace and security by misusing technology to harm individuals, disrupt communities, and erode ethical and moral principles. **Verse 51** condemns those who spread corruption, which parallels digital terrorism that endangers societal peace and security. Such acts involve the misuse of technology to harm individuals, destabilize communities, and undermine ethical values, highlighting the destructive consequences of exploiting digital platforms for malicious purposes. **Verse 90**: "O believers! Intoxicants, gambling, idols, and drawing lots for decisions are all evil of Satan’s handiwork. So, shun them so you may be successful." This verse emphasizes the need to avoid harmful actions, which can encompass participating in or endorsing digital terrorism. It underscores the importance of refraining from behaviors that jeopardize societal well-being and disrupt peace through the misuse of technology.

These verses collectively emphasize the foundational values of justice, accountability, and the protection of life and societal welfare. These principles are not only central to Islamic teachings but are also crucial in addressing modern issues like digital terrorism. Digital terrorism, which often exploits technology to cause harm, destabilize societies, and undermine moral values, directly conflicts with the objectives outlined in

these verses. By stressing the need for fairness, responsibility, and the safeguarding of peace, these verses provide clear guidance on how to approach and mitigate the dangers posed by such malicious actions. Upholding these principles ensures that technology is used ethically and responsibly, fostering security, stability, and the well-being of society.

Surah Al-Hujurat also highlights themes of social ethics, the necessity of verifying information, and the repercussions of spreading falsehoods, all of which are relevant to the issue of digital terrorism. It emphasizes the importance of truthfulness and accountability in preventing harm in both social and digital spheres. **Verse 6 of Surah Al-Hujurat** says that "O you who have believed, if there comes to you a disobedient one with a report, investigate, lest you harm a people out of ignorance and become, over what you have done, regretful." This verse highlights the importance of verifying information before acting, a crucial step in combating misinformation and disinformation that can incite or fuel digital terrorism. These verses collectively emphasize the significance of ethical conduct, the verification of information, and promoting respect within communities—essential elements in tackling the challenges posed by digital terrorism.

Conclusion

In conclusion, countering digital terrorism in Pakistan is an urgent and multifaceted challenge that requires a comprehensive and coordinated approach. As the digital landscape continues to evolve, so too do the tactics employed by extremist groups seeking to exploit technology for their nefarious purposes. The increasing frequency of cyber-attacks, coupled with the vulnerabilities inherent in Pakistan's cybersecurity infrastructure, underscores the need for immediate action. To effectively counter digital terrorism, Pakistan must adopt a multifaceted approach that includes strengthening its cybersecurity infrastructure, enhancing legal frameworks, and fostering public awareness about the risks associated with online radicalization. International collaboration is also essential for sharing best practices and resources to combat this transnational threat. In conclusion, conceptualizing digital terrorism in Pakistan requires a nuanced understanding of its implications for national security, civil liberties, and social cohesion. As the country navigates this complex landscape, it must balance the need for security with the protection of democratic values, ensuring that responses to digital threats do not infringe upon fundamental rights. Preventive measures rooted in Islamic teachings—such as promoting ethical behavior online, fostering digital literacy, and encouraging responsible use of technology—are essential to counteract the spread of extremist ideologies. Moreover, the emphasis on collective responsibility (mas'ooliyyah) within Shariah calls for collaborative efforts among

individuals, communities, and governments to create a secure digital environment. Furthermore, as highlighted by leaders like General Asim Munir, it is crucial to verify information before dissemination to prevent the spread of falsehoods that can lead to societal discord. Engaging in constructive dialogue and implementing educational programs can help mitigate the risks associated with digital terrorism while reinforcing social cohesion. Ultimately, a comprehensive strategy that combines preventive measures with restorative justice, grounded in Shariah principles, can effectively address the complexities of digital terrorism while ensuring the welfare and security of society as a whole. By addressing these challenges head-on, Pakistan can better safeguard its digital environment while fostering a more resilient society capable of resisting extremist narratives.

Recommendations

Here are some recommendations for countering digital terrorism in Pakistan:

- Finalize the establishment of a dedicated National Cybersecurity Authority to oversee and coordinate cybersecurity efforts across all sectors, ensuring a unified response to digital threats.
- Invest in upgrading cybersecurity infrastructure for both government and private sectors, focusing on deploying advanced security technologies and protocols to protect critical data and systems.
- Implement training programs and partnerships with educational institutions to cultivate a skilled workforce in cybersecurity. This includes creating specialized degree programs and certification courses to address the shortage of professionals in the field.
- Update and enforce legal frameworks related to cybercrime and data protection. This includes strengthening laws under the Prevention of Electronic Crimes Act (PECA) to ensure effective prosecution of cyber offenders.
- Launch nationwide campaigns to educate citizens about cybersecurity risks, safe online practices, and the importance of reporting suspicious activities. Increased awareness can empower individuals to protect themselves against digital threats.
- Engage in international partnerships with other countries and organizations to share intelligence, best practices, and resources for combating digital terrorism. Participation in global cybersecurity forums can enhance Pakistan's capabilities.
- Develop comprehensive incident response plans for both public and private sectors to ensure quick and effective responses to cyber incidents. Regular drills and simulations can help prepare organizations for potential attacks.
- Invest in research and development initiatives focused on cybersecurity technologies. Establish public-private partnerships to foster innovation and create indigenous solutions tailored to local challenges.

- Establish clear data governance policies that outline responsibilities for data protection, access controls, and breach notification procedures. This will help organizations manage sensitive information more effectively.
- Continuously monitor the evolving cyber threat landscape using advanced analytics and threat intelligence tools. This proactive approach can help identify potential vulnerabilities before they are exploited.

By implementing these recommendations, Pakistan can strengthen its defenses against digital terrorism, safeguard its critical infrastructure, and promote a secure digital environment for its citizens.

Bibliography

Adil Adeel, and Rafi us Shan. "Global Cyber Terrorism: Pakistan's Cyber Security in Perspective." Pakistan Journal of Terrorism Research 2, no. 1 (2021). https://nacta.gov.pk/wp-content/uploads/2021/09/Global-Cyber-Terrorism.pdf.

Ahmad, Syed Bilal, and Dr. M. Sheharyar Khan. "Cyber Threat to Pakistan National Security: National Security and Threat Perception." Pakistan Review 3, no. 1 (2022): 1-10. https://www.pakistanreview.com/index.php/PRSS/article/download/142/94/471.

Basit, Abdul. "Digital Terrorism: A Label to Stifle Pakistan's Political Opposition?" The Diplomat, July 29, 2024. https://thediplomat.com/2024/07/digital-terrorism-a-label-to-stifle-pakistans-political-opposition/.

Denning, Dorothy E. "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives." Focus on Terrorism 9 (2000): 71-76.

Economic Times. "Pakistani Netizens Being 'Walled Off' as Army Shifts Focus to 'Digital Terrorism'." September 2, 2024. https://economictimes.indiatimes.com/news/defence/pakistani-netizens-being-walled-off-as-army-shifts-focus-to-digital-terrorism/articleshow/113001392.cms.

Hussain, Iftikhar, and Malik Waqar Ahmed. "Digital Terrorism Spurs Debate on Social Media Use in Pakistan." South and Central Asia, August 27, 2024. https://www.voanews.com/a/digital-terrorism-spurs-debate-on-social-media-use-in-pakistan/7759300.html.

Imran, Muhammad, and Ghulam Ali. "The Rise of Cyber Crime in Pakistan: A Threat to National Security." Journal of Development and Social Sciences 3, no. 4 (October-December 2022): 631-640. http://dx.doi.org/10.47205/jdss.2022(3-IV)58.

Kenney, Michael. "Cyber-Terrorism in a Post-Stuxnet World." Orbis 59, no. 1 (2015): 111–128. https://doi.org/10.1016/j.orbis.2014.11.009. This entry includes the author, title, journal name, volume and issue number, publication year, page range, and DOI link.

Masood, Awais. "'Digital Terrorism': A Label to Stifle Pakistan's Political Opposition?" The Diplomat, July 23, 2024. https://thediplomat.com/2024/07/digital-terrorism-a-label-to-stifle-pakistans-political-opposition/.
Sahar, Saba, and Areesha Anwer. "Cyberwarfare: A Threat to National Security." Pakistan Journal of Terrorism Research 4, no. 1 (2021). https://nacta.gov.pk/wp-content/uploads/2021/09/Dr.-Saba-Sahar-Areesha-Anwer.pdf.
Theohary, Catherine A., and John W. Rollins. "Cyberwarfare and Cyberterrorism: In Brief." Congressional Research Service, March 27, 2015. https://sgp.fas.org/crs/natsec/R43955.pdf. This entry includes all necessary details such as the authors, title, publication source, date, and URL.
United Nations Security Council Counter-Terrorism Committee Executive Directorate. "Counter-Terrorism in Cyberspace." October 2021. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct_2021.pdf.
Weimann, Gabriel. "Cyberterrorism: How Real Is the Threat?" Special Report 119. United States Institute of Peace, December 2004. https://www.usip.org/sites/default/files/sr119.pdf.
Zeiger, Sara, and Joseph Gyte. "Prevention of Radicalization on Social Media and the Internet." In Handbook of Terrorism Prevention and Preparedness. https://www.icct.nl/sites/default/files/2023-01/Chapter-12-Handbook_0.pdf.

Referenses

[1] Adil Adeel and Rafi us Shan, "Global Cyber Terrorism: Pakistan's Cyber Security in Perspective," Pakistan Journal of Terrorism Research, Vol II, Issue I, https://nacta.gov.pk/wp-content/uploads/2021/09/Global-Cyber-Terrorism.pdf
[2] Catherine A. Theohary and The Ind John W. Rollins, "Cyberwarfare and Cyberterrorism: In Brief," Congressional Research Service, March 27, 2015, https://sgp.fas.org/crs/natsec/R43955.pdf.
[3] Kenney M. 2015. Cyber-terrorism in a post-stuxnet world. Orbis 59(1):111–128, DOI10.1016/j.orbis.2014.11.009
[4] D. E. Denning, "Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives," Focus on Terrorism, vol. 9, 2000.
[5] Abdul Basit, "Digital Terrorism': A Label to Stifle Pakistan's Political Opposition?," The Diplomat, July 29, 2024, https://thediplomat.com/2024/07/digital-terrorism-a-label-to-stifle-pakistans-political-opposition/
[6] Iftikhar Hussain and Malik Waqar Ahmed, "Digital terrorism' spurs debate on social media use in Pakistan," South and Central Asia, August 27, 2024,

https://www.voanews.com/a/digital-terrorism-spurs-debate-on-social-media-use-in-pakistan/7759300.html.

[7] Gabriel Weimann, "Cyberterrorism How Real Is the Threat?," United States Institute of Peace, Special Report 119, December 2004, https://www.usip.org/sites/default/files/sr119.pdf

[8] Sara Zeiger and Joseph Gyte, "Prevention of Radicalization on Social Media and the Internet," Handbook of Terrorism Prevention and Preparedness, https://www.icct.nl/sites/default/files/2023-01/Chapter-12-Handbook_0.pdf

[9] "Preventing Violent Extremism through Promoting Inclusive Development, Tolerance and Respect for Diversity: A Development Response to Addressing Radicalization and Violent Extremism, "United Nations Development Programme, 2016, https://www.undp.org/sites/g/files/zskgke326/files/publications/Discussion%20Paper%20-%20Preventing%20Violent%20Extremism%20by%20Promoting%20Inclusive%20%20Development.pdf

[10] Saba Sahar and Areesha Answer, "Cyberwarfare: A Threat to National Security," Pakistan Journal of Terrorism Research, Vol 04, Issue-1 (2021), https://nacta.gov.pk/wp-content/uploads/2021/09/Dr.-Saba-Sahar-Areesha-Anwer.pdf.

[11] Iftikhar Hussain and Malik Waqar Ahmed, "Digital terrorism' spurs debate on social media use in Pakistan," South and Central Asia, August 27, 2024, https://www.voanews.com/a/digital-terrorism-spurs-debate-on-social-media-use-in-pakistan/7759300.html.

[12] Abdul Basit, "Digital Terrorism': A Label to Stifle Pakistan's Political Opposition?," The Diplomat, July 29, 2024, https://thediplomat.com/2024/07/digital-terrorism-a-label-to-stifle-pakistans-political-opposition/

[13] Iftikhar Hussain and Malik Waqar Ahmed, "Digital terrorism' spurs debate on social media use in Pakistan," South and Central Asia, August 27, 2024, https://www.voanews.com/a/digital-terrorism-spurs-debate-on-social-media-use-in-pakistan/7759300.html.

[14] Nawal Munir Ahmad, "The Evolution of Internet Governance: Shaping Pakistan's Digital Future," NetMission Insights, June 27, 2024, https://netmission.asia/2024/06/27/the-evolution-of-internet-governance-shaping-pakistans-digital-future-nawal-munir-ahmad/.

[15] Robert W., Taylor, Eric J. Fritsch, and John Liederbach, Digital crime and digital terrorism, Prentice Hall Press, 2014.

[16] Gabriel Weimann, Terrorism in cyberspace: The next generation, Columbia University Press, 2015.

[17] "Cyber threats increased by 17% in 2023," The Express Tribune, October 11, 2024, https://tribune.com.pk/story/2457021/cyber-threats-increased-by-17-in-2023

[18] "Spyware attacks increased by 300% in Pakistan," The Express Tribune, May 10, 2024, https://tribune.com.pk/story/2466023/spyware-attacks-increased-by-300-in-pakistan.
[19] "Cyber threats increased by 17% in 2023," The Express Tribune, October 11, 2024, https://tribune.com.pk/story/2457021/cyber-threats-increased-by-17-in-2023
[20] Abeera Haider etal, "Use of Facebook and Twitter by Terrorist Organizations to Radicalize the Youth: A Case Study of TTP, BLA and ISIS in Pakistan," Bulletin of Business and Economics,12(2), 171-177, file:///C:/Users/abdul/Downloads/465-Article+Text-1290-1-10-20230915.pdf.
[21] Ibid.
[22] "Pakistani netizens being 'walled off' as army shifts focus to 'digital terrorism," The Economic Times, September 02, 2024, https://economictimes.indiatimes.com/news/defence/pakistani-netizens-being-walled-off-as-army-shifts-focus-to-digital-terrorism/articleshow/113001392.cms
[23] Abeera Haider etal, "Use of Facebook and Twitter by Terrorist Organizations to Radicalize the Youth: A Case Study of TTP, BLA and ISIS in Pakistan," Bulletin of Business and Economics,12(2), 171-177, file:///C:/Users/abdul/Downloads/465-Article+Text-1290-1-10-20230915.pdf.
[24] "Kaspersky on Pakistan landscape: Number of cyber threats rose by 17pc in 2023," Business Recorder, February 20, 2024, https://www.brecorder.com/news/40289669.
[25] "Spyware attacks increased by 300% in Pakistan," The Express Tribune, May 10, 2024, https://tribune.com.pk/story/2466023/spyware-attacks-increased-by-300-in-pakistan.
[26] Andrew M. Colarik, Cyber terrorism: political and economic implications, Igi Global, 2006.
[27] Stefano Baldi, Eduardo Gelbstein, and Jovan Kurbalija. Hacktivism, cyber-terrorism and cyberwar: The activities of the uncivil society in cyberspace, Diplo Foundation, 2003.
[28] Salman Siddiqui, "Pakistan to establish cybersecurity authority," The Express Tribune, July 26, 2024, https://tribune.com.pk/story/2483019/pakistan-to-establish-cybersecurity-authority.
[29] "National Cyber Security Policy 2021," Ministry of Information Technology & Telecommunication, Government of Pakistan, July, 2021, https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf
[30]The prevention of electronic crimes act, 2016, Ministry of Law and Justice, https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%253D-sg-jjjjjjjjjjjj
[31] PTA Issues Cyber Security Strategy 2023-2028 for Pakistan's Telecom Sector:

A Five Year Plan Towards Digital Resilience, Pakistan Telecommunication Authority, https://www.pta.gov.pk/category/pta-issues-cyber-security-strategy-2023-2028-for-pakistans-telecom-sector-a-five-year-plan-towards-digital-resilience-980103515-2024-07-04#:~:text=The%20strategy%20is%20built%20on,and%20collaboration%2C%20and%20public%20awareness.

[32] Muhammad Riaz Shad, "Cyber threat landscape and readiness challenge of Pakistan," Strategic Studies 39, no. 1 (2019): 1-19.

[33], Muhammad Zia Ur Rehman, Waseem Ishaque, and Mr Hamza Amir Khalil Sayed, "Emerging Dynamics and National Security of Pakistan: Challenges and Strategies," Research Consortium Archive 3, no. 1 (2025): 228-240.

[34] "Enhancing Pakistan's Capacity for Managing Electronic Evidence with Denmark's Support," Office on Drugs and Crime Country Office Pakistan, United Nations, https://www.unodc.org/copak/en/Stories/SP4/enhancing-pakistans-capacity-for-managing-electronic-evidence-with-denmarks-support.html.

[35] Peter Romaniuk, Multilateral counter-terrorism: the global politics of cooperation and contestation, Routledge, 2010.

[36] Anthony H. Cordesman, "Islam and the Patterns in Terrorism and Violent Extremism," Centre for Strategic and International Studies, October 17, 2017, https://www.csis.org/analysis/islam-and-patterns-terrorism-and-violent-extremism