AMCAP | JMCS

AMCAP JMCS |
JOURNAL OF MEDIA AND COMMUNICATION STUDIES
Volume 5, Issue 1. January 2025

DOI: 10.5281/zenodo.14620050.

Website home: https://jmcs.amcap.net/website
Submission guidelines: https://jmcs.amcap.net/website/page/submission-guidelines

Date of Receiving: 10/9/2024
Date of Acceptance: 08/28/2024
Date of Publication: 01/10/2025

Digital Terrorism: Impacts and Outcomes for Pakistan

Author(s):

Qazi Muhammad Shahzad Khalil
Department of Political Science & International Relations, University of Management & Technology, Lahore.

Muhammad Imran
Department of Political Science & International Relations, University of Management & Technology, Lahore.
Email: manikasur2@gmail.com

Zoha Anjum
Forman Christian College University, Lahore.

Majid Mohsin
Department of Political Science & International Relations, University of Management & Technology, Lahore.

Abstract

A new form of threat is emerging in Pakistan along with the conventional form of terrorism and that is Digital terrorism which is affecting the social order of the society. This paper scrutinizes the influences and consequences of digital terrorism on Pakistan's socio-economic landscape, politics, and national security. It is exhibited through cyber-attacks on strategic installations, the spread of extremist ideology online, and the use of social media platforms for hiring and extremism. These events not only imperil national security but also undermine the country's economic growth by discouraging investor confidence and disturbing financial systems. Moreover, this threat worsens social tensions by nurturing sectarianism and expanding societal divisions. The paper examines the response mechanisms of the government of Pakistan and private sector to contest digital terrorism, including cyber security initiatives, legislative measures, and international collaborations. It also highlights the challenges in effectively countering digital terrorism, such as scientific boundaries, insufficient policy frameworks, and the complex interplay between freedom of expression and security. Eventually, the study calls for an inclusive and multi-faceted approach to address digital terrorism in Pakistan, emphasizing the need for improved public awareness, cyber security infrastructure, and regional cooperation.

Keywords: Digital Terrorism, Propaganda, Cyber Security, Social Media tools.

Introduction

Digital terrorism is a menace at home and as well as in developing and underdeveloped countries because it is actually a borderless entity. Terrorists exploit the secrecy and reach of the internet to spread fear, to intimidate populations, and to destabilize societies through fake publicity, disturbance of dangerous infrastructure, and incitement of ferocity. The misuse of cyberspace led to digital inventions and technologies cause digital terrorism. The repercussions can be dangerous as shown online hate speech that led to ethnic cleansing in Myanmar. Other examples are that of recent Bangladesh students uprising and foreign interference in last American elections. In addition, social media is also used for recruitment and spread their negative agenda across borders by international organization. This may increase the risk of global security threats to secure lands. Developing countries like Pakistan, where conventional methods of terrorism are prevalent, digital terrorism will create a new threat to the peace of state and it intensifies the fight against terrorism with more complexity. The accessibility of digital devices, tools has made it easier for the deviant organizations to plan attacks and spread fear and hatred among the people of state. Lastly, Pakistan can address this new form of terrorism by developing a national strategy which outlines pragmatic steps to counter online propaganda, strategic installations and promote media education. Similarly, the training and resources for cyber security professionals is also important along with technology transfer from China and the USA. In a nut shell, this research aims to understand the impact and influence of digital terrorism in Pakistan with a focus on its socio-political outcomes and the measures being taken to address this threat.

Problem statement

Pakistan is facing an increasingly serious threat from digital terrorism, which is the use of cyberspace and digital platforms by terrorist groups to spread propaganda, recruit new members, encourage extremism, and launch cyber threats. The nation now faces the challenge of fighting digital extremism, which has no borders and is harder to identify and combat, in addition to traditional forms of terrorism. Cyber terrorism has had a number of effects on Pakistan. It has radicalized people, particularly young people, through internet propaganda.There is a direct threat to national security as more and more Pakistanis are being recruited by extremist organizations through social media and other digital platforms. Cyber threats on government agencies, private businesses, and vital infrastructure also have the ability to destabilize the nation.

Literature review

Digital terrorism, also referred to as cyber terrorism, covers the use of digital platforms and cyberspace by terrorist organizations to further their plans. This phenomenon has significant implications for national security, especially in countries like Pakistan, which has been a focal point of regional and global terrorist activities. The literature on cyberterrorism scrutinizes its origin, ways, influences, and the countermeasures adopted by states. This assessmentblendsprevailing research on the impacts and outcomes of digital terrorism in Pakistan.Due to the accessibility of the internet and technological advancements, digital terrorism has emerged at global and domestic arena. Existing literature concentrated on the use of the internet by terrorist organization for communication, employment, and misinformation (Weimann, 2004). Sophisticated cyber-attacks, online radicalization, and the use of social media platforms have expanded the incitement and violent activities over the passage of time. (Conway, 2012).For an underdeveloped country like Pakistan, the rise of digital terrorism is linked to the wider socio-political scene. In the realm of digital terrorism, Pakistan's involvement in the global “War on Terror” and its internal struggles with extremist groups has made it a significant target and participant for cyber attackers and propagandists. As shown in the numerous studies, different splinters terrorist groups such as Tehrik-i-Taliban Pakistan (TTP) and Lashkar-e-Taiba (LeT) have utilized online platforms to coordinate attacks, disseminate false information, and recruit personnel (Khan, 2017).

Research questions

1. In what ways has the emergence of digital terrorism affected the recruitment and indoctrination of extremist groups in Pakistan, and what steps might be taken to counter these trends?
2. How effectively do the country's current risk-reduction policies address the socioeconomic and security effects of cyber-attacks associated with digital terrorism on Pakistan's vital infrastructure?

Theoretical background

Barry Buzan's Securitization Theory, a core theory within the Copenhagen School of thought, is the base of this study on digital terrorism in Pakistan. According to securitization theory, issues can become security concerns through the articulation of these issues as such by political leaders, institutions or media. This theory is most relevant to digital terrorism, a domain which they refer to as a place where nontraditional security threats like cyber attacks and online radicalization are framed as important for national security. However, articulation of digital terrorism as a security threat calls for extraordinary measures, and this theory is ideal for the analysis of Pakistan's response to threats of this nature.

Securitization of Cyberspace: The concept of securitization by Buzan is very applicable in cyberspace domain, where it constructs the security threat of digital terrorism. Seas visions and perceptions securitized Pakistan's digital platforms, particularly consumption of its critical infrastructure, enough extremist ideologies, manipulation of public discussion through online propaganda. Framing cyberspace as a national security problem is not only a call for mobilization of resources but also of justification of curtailment of digital freedoms, which in turn opens ethical and governance issues.

Cyber Deterrence Theory: Cyber deterrence theory, which focuses on deterring or mitigating cyber threats, is another relevant theoretical framework. Cyber-attacks on strategic installations constitute digital terrorism which can be counteracted through mechanisms of deterrence of cyber terrorism such as a robust cyber defense an infrastructure that can as well be backed up by an international cooperation that can yield punitive measures against offenders among others. Similar to this theory, Pakistan is working towards making cyber initiatives and legislative frameworks more robust which can prevent terrorist utilization of digital platforms.

Social Constructivism in Cyberspace: Using the social constructivist theory, the role of ideas, beliefs and identities in shaping human interactions and societal structures come to focus. The internet has become the medium through which extremist narratives, sectarian divides and social tensions are built and disseminated when viewed in the context of digital terrorism. The social constructivism demonstrates how terrorist groups recruit people and disguise with agenda by using societal constructs for the advantage of themselves, mainly of the youth. It is important to understand these processes in order to come up with counter narratives that counter the extremist ideologies.

The theoretical perspectives are integrated to understand the complex phenomenon of digital terrorism in Pakistan. A comprehensive framework, and thereby an analysis of the socio political and economic implications of digital terrorism, and the effectiveness of countermeasures can be examined after exploring the interplay between securitization, deterrence and social constructivism. The significance of long-term solutions across policy frameworks, technology, and societal resilience to counter the shifting threat of digital terrorism is also highlighted.

Methodology

This research adopts a qualitative design to investigate impact of digital terrorism on Pakistan's socio-economic outlook, politics and national security. The research is based on secondary data sources and uses systematic analysis to gain insights into the complex dynamics of digital terrorism.

Research Design: The investigation is a qualitative, the review studies and case studies were selected for critical assessment of the digital terrorism phenomenon. Using this approach, a more in depth understanding of the subject area is achieved through the synthesis of information from existing literature, reports and documented incidents.

Data Collection: The sources of data for this research consists of only secondary sources that are broad and rich including. These sources include:

- Journal peer reviewed articles
- Books and academic papers.
- Reputable magazines and news articles
- Although government and international organizations have issued reports.
- Search the online databases and accessible internet sources.

The secondary data of this research is broad spectrum which means that the research would capture a lot of peoples' perspectives or insight on the subject.

Data Analysis: The data is analyzed using qualitative methods, primarily:

- Review Studies: Digital terrorism, the use of digital technology to conduct terrorist activity, has been examined systematically, reviewing existing theoretical frameworks, case studies and policy analyses. This method does then make it possible to identify patterns, themes and gaps in the current understanding of the phenomenon.
- Case Studies: To offer contextual and empirical counter evidence, specific instances of digital terrorism in Pakistan and globally are analyzed. As case studies, cyber attacks on critical infrastructure, digital spread of online radicalization campaigns, social media recruitment by extremist groups are presented to demonstrate the practical aspects of digital terrorism.

Methodological Rigor: To ensure the reliability and validity of the findings, the study incorporates the following measures:

- When making an entry, cross referencing the data to see that the information is accurate and consistent between all sources.
- Thematic analysis to identify repeating patterns and key themes in the literature and case studies.
- Evaluating the credibility and relevance of sources critically, giving priority to peer reviewed and high impact publications.

Scope and Limitations: The methodology used yields useful results, but the reliance on secondary data could prevent the ability to take advantage of the immediacy of developments or stakeholders' perspectives in countering digital terrorism. This study could be complemented in future research by including primary data in the form of interviews, surveys, or focus groups.

Results and discussion

1. **The Landscape of Digital Terrorism in Pakistan:**
   - 1.1 **Forms of Digital Terrorism:** For enrollment and coordination, digital terrorism in Pakistan exhibits in several forms, including cyber-attacks, online radicalization, propaganda spreading, and the use of social media platforms
   - 1.2 **Cyber-attacks:** Terrorist organizations and their aides have remotely used cyber-attacks to attack strategic installations, government departments, and financial systems in Pakistan. These attacks focus to create distraction, spread fear, and fades away trust in the state's ability to protect its residents.
   - 1.3 **Online Radicalization:** The internet helps as a useful tool for the radicalization of people, particularly the youth. Radical ideologies are spread through social media, forums, and encrypted communication platforms, making it hard for experts to display and seize these activities.
   - 1.4 **Propaganda Dissemination:** Digital platforms are used widely to spread propaganda, glorify terrorism, and provoke violence. The reach of these platforms permits terrorist stances to spread rapidly and extensively, obscuring struggles to counter such messaging.
   - 1.5 **Recruitment and Coordination:** New members are recruited and coordinate attacks are carried out by terrorist groups using digital platforms. Encrypted messaging apps give a safe and secure media of communication, making it difficult for law enforcement agencies to spot and thwart potential threats.
   - 1.6 **Socio-political Impacts:** The socio-political impacts of digital terrorism in Pakistan are multifaceted which include polarization in the society. It is affecting various aspects of society and governance.
   - 1.7 **Polarization and Social Unrest:** Pakistani society is facing divide and polarization due to the fake media propaganda. Due to which social unrest is erupted, with different groups being eroded against each other based on spiritual, sectarian, or philosophical lines. The rise of digital echo chambers further aggravates these divisions, making it harder to achieve Hence, national unity is harder to achieve due to the division created in the society with rise of online media.

2. **Impacts on National Security and Society:** The consequences of digital terrorism on Pakistan are in multiple forms, affecting national security, social fabric, and financial stability. One of the main concerns is the threat to strategic installations, as terrorist group frequently hit networks of government and important services. Akbar (2020) highlights numerous cases where cyber-attacks interrupted military and governmental operations in Pakistan, showing the susceptibilities in the

country's cyber security structure. Furthermore, digital terrorism has intensified the radicalization of youth. Radical groups have been able to reach and have an impact on a larger audience thanks to the widespread use of social media and programmed messaging apps. This has prompted a rising worry about the radicalization of Pakistani youth, dominatingly in regions with lacking admittance to formal preparation and work potential open doors (Ahmad, 2019). Digital terrorism in Pakistan has exacerbated social polarization in addition to security threats. According to Saeed (2018), the online propagation of extremist ideologies has fueled sectarian violence and intolerance, further dividing Pakistani society along ethnic and religious lines. This polarity makes it stiffer to support peace and stability in the country and harms social cohesion.

3. **Challenges to Governance:** The governance in Pakistan faces momentous challenges as a result of digital terrorism. It is tough for the government to continue with the rapid development of digital threats, and the policies or law that are in place are often insufficient to deal with the densities of cyberspace. Resultantly, there has been criticism on the capacity of Government to maintain public order and security.

4. **Impact on International Relations:** Pakistan's image is commonly impacted by the assessment that it is a heart for automated psychological warfare. This has an impact on its international relations, particularly with states that are the targets of digital terrorist activities. Diplomatic relations are further complicated by the need to deal with the issues of privacy and freedom of speech dilemma on one hand, and fight against terrorism, on the other hand.

5. **Economic Outcomes:** Thus, it may be said that Pakistan is sort of influencing by the monetary effects of computerized oppression. Digital related attacks disrupt organizations and basic foundation, resulting to more losses in terms of money. The actual spending on cyber security and protection from terrorism takes lots of money which are siphoned from productive areas like education and health. In addition, the depiction of Pakistan as an intentionally unsure state undercuts its perception for new image and impacts the monetary advancement.

6. **Countermeasures and Strategies:**

   6.1 Government Initiatives: The government of Pakistan has enacted various measures to deal with the menace of cyber terrorism some of which include establishing special cybercrimes wings and the Prevention of Electronic Crimes Act (PECA) that was passed in 2016 with a view of enhancing the support structure for efficient cyber security. Such activities are expected to re-emphasize the defenses of the state when it comes to addressing digital threats as well as outline a legal framework for handling cybercrime.

   6.2 Role of Technology and International Cooperation: Fighting digital terrorism needs technology because terrorists use technology to conduct their activities in the cyber world. Pakistan is at last starting to spend money on advanced tracking and spying systems with a view to combating cyber and net radicalization. However, development and update are this necessary because of the changes that occur in the technological world which poses a threat to computers. Thus, it is also needed the international cooperation in combating with cyber terrorism. Since the struggle against digital terrorism has the international aspect Pakistan's cooperation with other countries in terms of information exchange and joint cyber security drills are critical. Besides, working with global firms in technology can help in preventing dissemination of extremism over the internet by meeting legal standards that is allowable in the area.

6.3 Governmental and Institutional Responses: Being aware of the potential of cyber terrorism, the Pakistani government has drawn certain measures as follows. To address these threats, these actions include establishing cybercrime units, passing network protection regulation, and engaging internationally. Some of the legal measures include the Prevention of Electronic Crimes Act (PECA) of 2016 whereby, among other things, cyber terrorism is prohibited (Rehman, 2017). This indicate that it is still very hard to effectively counter cyber terrorism despite these measures. The critics argue that policing institutions have lacked adequate resources and professional support for providing appropriate resources and technical support for enabling the police forces to effectively and fairly apply cyber security across the countries (Shah, 2021). besides, relations between the private and the public sectors should be more symbiotic, for instance in making core infrastructures more secure against cyber threats.

7. **Outcomes and Future Directions:** They have numerous impacts in Pakistan which vary with time though they all fall under the category of cyber terrorism. Since cyber attacks are nowadays a fluid type of threat, it is regrettable but true that even if the nation has advanced in the fight against the hostile activity, a number of new issues emerge periodically. As per findings, it holds the call to enhance a strong cyber security regime apart from doing better job to minimize the impact of cyber threats, Pakistan should establish a stronger strategy that works for the factors provoking extremism in the country, including poverty, social disparity, and restricted access to education (Yousafzai, 2020). Potential research areas regarding cyber based counter terrorism, role of international cooperation, and long term social political consequence digital terrorism in Pakistan need to researched in future. In addition, quantitative research evaluating the psychological impacts of cyber psychological warfare on the community with particular focus on youths and the role played by tertiary institutions in developing the ability to counter misleading accounts on the social media platforms.

8. **Challenges in Implementation:** In any case, different obstacles are still there in the way of Pakistan's efforts to counter the digital psychological operation effectively. Some of them are lack of adequate funding, inefficient administrative structures and low public awareness on the risks associated with cyber terrorism. Moreover, it remains unclear, whether the government has adequate tools to protect civil liberties and the right to free speech in their fight against terrorism initiatives.

Conclusion

The threat of digital terrorism to Pakistan is diverse and evolving and if not addressed it may have immense repercussions for the country's sociopolitical scenario and economy. The government has made an effort to solve this issue, however, there is much to do to develop technologies, to expand international collaboration and to align laws and regulations. It would be critically important in the future to continue the inclusive approach and to develop even stronger international cooperation, solid cyber security and public education in order to minimize the impact of digital terrorism to Pakistan. Digital terrorism affects the overall security of Pakistan and lowers the social morale and purchasing power parity in the country and also raise critical problems for the nation. Still, Pakistan has tried to counter this threat based on the existing research, but to eliminate the reasons behind the increase of the digital terrorism more works is needed. The digital terrorism in Pakistan cannot be mitigated by the cyber security measures only but there is a need to introduce social and economic changes at the same time.

References

Abbas, H. (2017). Pakistan’s counterterrorism strategy: Analysing successes and failures. *Asian Security, 13*(2), 89–111.

Ahmad, N. (2019). Digital radicalization in Pakistan: The role of social media in recruiting extremists. *Journal of Terrorism Studies, 3*(1), 45–67.

Ahmed, I. (2021). The digital battleground: Cyber extremism in South Asia. *Cyber Studies Journal, 5*(1), 34–50.

Akbar, M. (2020). Cyber-attacks on critical infrastructure: The case of Pakistan. *International Journal of Cybersecurity, 8*(2), 101–115.

Ali, M. (2019). Social media and terrorism: The changing dynamics in Pakistan. *Journal of Contemporary South Asian Studies, 18*(2), 99–123.

Aziz, F. (2020). Cybersecurity threats in South Asia: Implications for Pakistan’s security. *Asian Journal of Security Studies, 14*(3), 203–221.

Aziz, M. (2021). The impact of digital terrorism on Pakistan’s economy. *Pakistan Journal of Economic Studies, 14*(2), 23–39.

Bhattacharjee, A. (2020). Cyber warfare and national security: A case study of South Asia. *Journal of Political Science, 16*(4), 76–95.

Brown, A. R. (2015). The role of social media in modern terrorism. *Journal of Security and Strategy, 9*(3), 45–66.

Conway, M. (2012). From al-Qaeda to ISIS: A history of terrorist propaganda on the Internet. In A. Silke (Ed.), *Handbook of terrorism research* (pp. 427–446). Routledge.

Hussain, K. (2020). Cyber laws in Pakistan: Challenges and opportunities. *Pakistan Journal of Legal Studies, 8*(1), 112–132.

Iqbal, S. (2022). Digital propaganda: Understanding extremist narratives in Pakistan. *Media and Communication Journal, 7*(2), 89–109.

Khan, F. (2017). Digital terrorism and extremism in Pakistan: A case study of Tehrik-i-Taliban Pakistan. *Pakistan Journal of International Affairs, 10*(1), 30–50.

Khan, H. (2020). Cybersecurity in Pakistan: A strategic overview. *National Institute of Pakistan Studies.*

Khan, M. (2021). Cybercrime and digital terrorism in Pakistan: Trends and responses. *Journal of Asian Security, 15*(1), 78–93.

Malik, R. (2019). Countering digital terrorism: Pakistan's cybersecurity initiatives. *Defense Policy Journal, 10*(3), 213–229.

Mehmood, A. (2020). Understanding digital terrorism: Lessons from Pakistan. *Journal of Counterterrorism Studies, 6*(4), 56–79.

Qureshi, H. (2021). The rise of cyberterrorism in Pakistan: Policy gaps and future prospects. *Pakistan Journal of Policy Research, 9*(2), 133–152.

Raza, S. (2020). Cyberattacks on Pakistan's financial sector: Challenges and countermeasures. *Journal of Economic Security, 5*(3), 98–114.

Rehman, H. (2017). The Prevention of Electronic Crimes Act: An analysis. *Pakistan Law Review, 22*(3), 214–237.

Roberts, T. (2018). Global cyber threats and their impact on developing nations. *Journal of Global Security Studies, 12*(1), 67–82.

Saeed, S. (2018). Sectarianism and the role of digital media in Pakistan. *Journal of Social Research, 14*(3), 199–218.

Shah, A. (2021). Challenges in implementing cybersecurity measures in Pakistan. *Journal of Defense Studies, 17*(2), 55–74.

Sharma, P. (2019). Cybersecurity and counterterrorism: A South Asian perspective. *Asian Journal of Security Studies, 13*(2), 77–96.

Siddiqui, M. (2021). Cybersecurity and its role in countering extremism in Pakistan. *Journal of Regional Security Studies, 11*(3), 211–229.

Weimann, G. (2004). Cyberterrorism: How real is the threat? *United States Institute of Peace.*

Williams, J. (2017). The evolving threat of cyberterrorism: Policy and practice. *Cyber Policy Review, 8*(2), 88–106.

Yamin, T. (2019). The role of technology in counterterrorism efforts in Pakistan. *Journal of Strategic Security, 12*(1), 45–67.

Yousafzai, Z. (2020). Addressing the root causes of extremism in Pakistan: The role of education and economic development. *Journal of Peace and Conflict Studies, 12*(1), 67–89.

Zahid, F. (2018). Radicalization and online extremism in Pakistan. *Institute for Policy Reforms.*