Orient Research Journal of Social Sciences *ISSN Print 2616-7085*
December, 2023, Vol. 8, No. 2 [01-09] *ISSN Online 2616-7093*

Triangle of Cyber Technology, Online Radicalization and Cyber Terrorism in Pakistan

Saqib Khan Warraich*[1] Abeera Haider[2] Dr. Alishba Mukhtar[3]

1. Assistant Professor, Department of political science, Government College University Lahore, Punjab, Pakistan
2. Lecturer, Department of Political Science, Queen Mary College, Lahore, Punjab, Pakistan
3. Medical Officer, DHQ M. B. Din, Punjab, Pakistan

***Corresponding Author:** dr.saqibkhan@gcu.edu.pk

Abstract

This study explores the influence of cyber technology on the phenomena of radicalization and terrorism in Pakistan, a country that has already been grappling with various forms of terrorism by state and non-state actors. The investigation employs both positivist and constructivist approaches to examine the impact of cyber technology on the promotion of radicalization and cyber terrorism in Pakistan, the reasons behind the emergence of radicalization and cyber terrorism, and potential remedies. Nowadays, most scholars agree that the cyber domain can be used to generate finances, propagate information, recruit individuals, and serve as an important tool in arriving at firefight. According to former CIA operations officer, Marc Sagerman, online radicalization has been replaced by face-to-face radicalization.

Key Words: Cyber Technology, Cyber Terrorism, Online Radicalization, Pakistan, Terrorism

Introduction

The rise of cyber technology has transformed the world, fostering global connections and promoting a sense of unity. Nonetheless, it has also introduced new threats, such as radicalization, terrorism, and destructive cyber tools. Terrorists are exploiting this technology to their advantage, using it to shut down networks at their discretion. Even large organizations such as Sony, Experian, and Blue Cross Blue Shield have fallen prey to cyber attacks, with three billion Yahoo email accounts being hacked, and the US Office of Personnel Management also falling victim to cyber terrorism. These incidents highlight the global state of cyber security, with no state being entirely immune to devastating cyber attacks and identifying cyber attackers is often difficult as they work anonymously and sometimes use nicknames. Loopholes in the system allow both state and non-state actors to sabotage and spy on targeted systems.

Pakistan is a country that has been struggling with terrorism for the past few decades, and the emergence of cyber terrorism has added to the difficulties faced by the government in dealing with this menace. The emergence of the IT sector in Pakistan has revolutionized the economy of the country but has also put the security of the cyber territory at risk due to the lack of awareness among users about potential threats. The scenario of conflict and trust deficit in South Asia has put Pakistan under constant pressure, and the use of innovative technologies has transformed the mode of warfare, making threats more severe in nature. Cyber attacks can be launched on communication systems or financial institutions by using cyberspace.

Moreover, a large number of youth in Pakistan are unaware of the term 'online radicalization', and government and academic institutions are not organizing awareness campaigns and programs on a regular basis. Resultantly, the youth can easily be lured by appealing terrorist websites, and they may respond to all messages without proper authentication and verification of contents. Security analysts in India have observed that educated youths are more productive than non-educated individuals for terrorist organizations, as they possess intriguing mastery that can underpin terrorist abilities in the cyber domain. Despite strict government measures, extremists are still maintaining contacts with global

terrorist groups and continually creating different virtual links, even influencing top-ranking dignitaries of the country.

This paper aims to explore the role of cyber technology in promoting radicalization and cyber terrorism in Pakistan, analyze the possible causes of radicalization and cyber terrorism in Pakistan, and propose solutions to counter these threats. Furthermore, the paper will examine the relationship between media and terrorism in Pakistan.

Difference between Cyber Terrorism, Cyber Warfare and Cyber Crime

It is necessary to distinguish between three distinct categories: cyber terrorism, cyber warfare, and cyber crime.

Cyber Terrorism

It refers to the use of digital attacks against IT devices and digital information with the intention of achieving specific social or political objectives. (Vasilescu, 2012)

Cyber Warfare

A nation's action aimed at causing damage to the computer systems of another country.

Cyber Crime

The utilization of computers to instigate illicit behaviors, such as digital stalking or digital provocation (Chupika & Juneau, 2016)

Literature Review

The rapid growth in interconnectivity and technological innovation has led to a significant shift from the physical to digital world. However, this shift has also created numerous vulnerabilities in the internet. To combat cyber terrorism in Pakistan, the Federal Investigation Agency (FIA), the Cyber Security Wing of NACTA, and the Pakistan Telecommunication Authority (PTA) are working together to enhance their capabilities.

Pakistan has emerged as a significant player in the digital economy, according to the United Nations, and has made strides in the field of information technology with the introduction of 3G, 4G, and 5G networks. However, Pakistan is also known to have a high concentration of malware hosting sites globally. In the first quarter of 2017, Pakistan recorded the second-highest malware encounter rate in the world at 27.48%. Microsoft has identified Pakistan as a primary target for malware attacks and cyber espionage. To counter these threats, Pakistan's Federal Investigation Agency (FIA) and the Cyber Security Wing of the National Counter Terrorism Authority (NACTA) are working together with the Pakistan Telecommunication Authority (PTA) to strengthen their capabilities in combating cyber terrorism. (Khattak, 2017)

According to the 2014 country rankings of internet users, Pakistan is listed among the top 20 nations with a total of 20,431,000 web users, and this number is continuously growing. In an article titled "Social, Digital and Mobile in Pakistan" by Simon Kemp, it is stated that there are currently 8,007,460 individuals from Pakistan who are active on social networking websites. Additionally, every 12 seconds, new users are joining Facebook from Pakistan. The number of Twitter users in Pakistan has also reached 3 million. (Siraj, 2018). According to data from August 2014, the proportion of Pakistani individuals using Facebook accounts for 8.3% of the country's total population. It can be inferred that Facebook is the primary social networking platform in Pakistan. (Haque, 2014)

According to the Anti-Phishing Working Group (APWG) report of 2020, cyber hackers initiated Distributed Denial of Service (DDoS) attacks on the websites of Pakistani Security Forces and Federal Government. The report highlighted the difficulty faced by the Federal Investigation Agency (FIA) in defending against such attacks, as it requires specialized training and expertise. The National Response Centre for Cyber Crime's official report further confirmed that FIA division lacked the ability to identify signs of intrusion, especially those conducted via proxies. (Bitaab, et al., 2020)

In Pakistan, the National Database and Registration Authority (NADRA) maintain and store all population-related information. Threat Track Security's report of 2014 ranked NADRA as one of the top institutions globally, making it a potential target for cyber-attacks. There is a possibility that hackers may hack confidential information of Pakistani citizens stored in NADRA. European countries use the Security Content Automation Protocol (SCAP) algorithm for their National Vulnerability Database (NVD) to enable effective security management. (Firdous, 2018)

Dr. Tughral Yamin, Associate Dean at the Center for International Peace and Stability (CIPS), National University of Sciences & Technology (NUST), expressed concern over Pakistan's slow response to cyber attacks. He in his article writes about how Pakistan is lagging behind to its neighboring countries like India and Iran. Dr. Yamin pointed out that Pakistan lacks a designated agency responsible for cyber security, and suffers from deficiencies in infrastructure and leadership. (Yamin, 2018)

Ammar Jaffri, a former additional director general at the Federal Investigation Agency (FIA), emphasized the need for a more proactive approach to cyber security. He cited Pakistan's low ranking in ICAN's (The Internet Corporation for Assigned Names and Numbers) cyber awareness index to support his argument. (Jaffri, Khan, & Lodhi, 2023)

During the year 2017, Pakistan was impacted by the WannaCry ransomware cyber-attack, which had already infiltrated 300,000 computer systems in 150 nations. (SADIA, Ali, & Tariq, 2022) The Ransomware virus is highly dangerous as it encrypts the data and renders it unreadable. This virus spreads through email attachments or software installation links, such as the WannaCry virus. Only the person who created the virus has the knowledge to decrypt the data, and demands payment in the form of bitcoins, which is an untraceable and advanced digital currency. Currently, one bitcoin is valued at $1,723, and the virus is rapidly spreading, affecting up to 5 million PCs per day (Nawazish, 2017). Consider the scenario where an unauthorized individual gains access to the databases of Islamabad and Punjab excise and taxation, and manipulates the records by designating non-taxpayers as taxpayers and vice versa. What if crucial infrastructures like power stations or NADRA's database get hacked? The potential consequences are endless, and the current state of affairs is unsettling.

Militant groups in Pakistan are actively using social media platforms such as Facebook and websites like 'Alqal online' to propagate their radical ideologies and recruit individuals. Groups such as Lashkar-e-Taiba, Jamat-ud-Dawa, Jaish-e-Muhammad, and Harkat-ul-Mujahideen use these platforms to focus on recruitment through innocent posts that eventually lead to the posting of jihadist material. These groups often use emotional messages and communicate in Urdu or Roman Urdu for local consumption. They also mix entertainment content with their extremist views, such as posting militant cartoons for children. Even though the Pakistani government has ordered these groups to shut down their websites, they resurface with anonymous identities. The primary focus of these groups is on recruitment, and Facebook is the most commonly used social media platform for this purpose. (Nawazish, 2017)

The Al-Faloja Islamic Forums boasts a vast following of more than 250,000 members, with the aim of spreading the Salafi-Jihadi message to Al-Qaeda sympathizers. In December 2008, they infiltrated Facebook and established supportive groups, which now have over 200 million active members. According to Pakistani authorities, in December 2016, five American Muslims were detained for enrolling online through YouTube and Facebook to communicate with terrorist organizations like

Lashker-e-Taiba and Lashkar-e-Jhangvi. The US Department of Homeland Security has asserted that online recruitment has escalated considerably with the rising use of Facebook and YouTube. The use of online linkages and communications, such as Facebook, presents Salafi-Jihadis with an opportunity to appeal to young Muslims and promote their ideology. An expert in analyzing jihadi's online networking, Abdul Hameed Bakir, has affirmed that Salafi-Jihadists utilize Facebook as a platform to disseminate their ideology. (al-Shishani, 2010)

Between 2012 and 2013, PTA (Pakistan Telecommunication Authority) blocked around 15,380 websites that were deemed to contain inappropriate content. Despite these efforts, the government has struggled to effectively restrict access to online radical content, as people have found ways to access blocked sites using proxy links. Extremist groups have been able to leverage cyber technology to influence and manipulate the public's opinions and beliefs. Alarmingly, less than 1% of Pakistan's financial resources are allocated towards the security of its cyber space. A study conducted by the Brookings Project in 2014 found that there were nearly 46,000 Twitter accounts controlled by ISIS. Between February and August 2016, about 235,000 Twitter accounts were shut down for promoting terrorism. An investigation by the Pakistani newspaper Dawn in 2017 found that out of the 64 extremist groups banned by the government, 41 were still active and using Facebook pages, groups, and individual user profiles to propagate radical content. The three largest profiles of extremist groups on Facebook in Pakistan are the Ahle Sunnat Wal Jammat (ASWJ), Jeay Sindh Muttahida Mahaz (JSMM), and Sipah-i-Sahaba Pakistan (SSP) (Rasool, 2015).

Online Radicalization and Cyber Terrorism

The proliferation of radicalization on the internet has become a widespread issue, and Pakistan is not immune to this trend. Extremist groups have been exploiting the internet to attract new members and spread their radical ideologies. Social media platforms, such as Facebook, Twitter, and YouTube, have become the preferred mode of communication for terrorist organizations. In Pakistan, groups like Tehreek-e-Taliban Pakistan (TTP) and Lashkar-e-Taiba (LeT) have leveraged social media to radicalize and recruit young individuals. Additionally, the internet has opened up new avenues for cyber terrorism, which involves utilizing digital technologies to carry out terrorist activities. The most common form of cyber terrorism involves launching cyber attacks to disrupt critical infrastructure. In Pakistan, cyber terrorism has emerged as a new threat to national security. The country has suffered numerous cyber attacks in recent years, targeting government websites, financial institutions, and utility companies. According to the FBI, cyber terrorism can inflict genuine physical harm and create panic among the masses. (Poduval, 2012) It is widely accepted among researchers that cyber terrorism shares similar characteristics with traditional terrorism in terms of its potential to cause harm. Like general terrorists, cyber terrorists are motivated by a desire to advance their religious, political, and ethnic ideologies. The primary difference between the two types of terrorists is the medium they employ to carry out their activities. While traditional terrorists seek media attention and public recognition by making threats to the general public, cyber terrorists prefer to operate in the shadows and remain hidden. Large-scale cyber-attacks can even have lethal consequences, underscoring the potential danger posed by cyber terrorism. Cyber terrorists are selective in choosing their targets, often targeting civilians in order to sow panic and create chaos in society. In the past, terrorist organizations were known to operate prominent websites that provided instructions on how to carry out Distributed Denial of Service (DDoS) attacks. In the present day, terrorists have adapted to modern technology and are leveraging cyber networks to expand their reach and influence. By utilizing the latest technology, they are able to threaten an increasing number of people. These terrorist groups are active in the cyber realm, seeking funding and support from sympathizers. Well-known organizations like ISIS and Al-Qaeda are employing social media and other websites to propagate their extremist ideologies. Furthermore, they are disseminating manuals that provide detailed information on how to use weapons such as rocket propelled grenades (RPGs) and suicide jackets. (Heickero, 2014)

Online material has a greater potential to radicalize individuals than traditional text-based materials. (Conway & McInerney, 2008) The topics of radicalization, terrorism, and the war against

terrorism are frequently discussed in social media. Reports from the European Union and the United Nations suggest that radicalization is a process that can lead to extremism and even terrorism According to a 2016 report by "We are Social," East Asia boasts the largest social media market, followed by Southeast Asia and North America. The report identifies Facebook and Facebook Messenger as the leading social and communication tools, with Twitter, Skype, Line, and WhatsApp following closely behind. Research indicates that online radicalization is a significant factor contributing to terrorism in China, particularly in the Xinjiang region. While local residents are not responsible for these attacks, outsiders who seek to separate Xinjiang from China are believed to be the culprits. Terrorists are leveraging television, radio, and the internet to spread their message. In Indonesia, the fourth-largest user of Facebook and the fifth-largest user of Twitter, the Institute for Policy Analysis of Conflict (IPAC) has noted that terrorists are increasingly utilizing social media platforms to communicate with young people. Recruitment efforts are conducted through propaganda videos on YouTube and online gaming platforms. The Indonesian government is taking the issue of online radicalization seriously. (Alava, Meigs, & Hassan, 2017)

In July 2011, the perpetrator of the Norway bombing and shooting, Anders Breivik, had been leading a reclusive lifestyle and was facing financial difficulties. He turned to playing video games as a form of escapism and ultimately decided to carry out the attacks as a martyr for his anti-Islamic beliefs. Similarly, Zachary Chesser underwent a radicalization process through online means after converting to Islam in the summer of 2008. He expressed support for terrorist groups and sought guidance from Anwar al Awlaki's sermons. In 2010, Chesser uploaded a video in which he threatened the creator of a television show that depicted the Prophet Muhammad (PBUH) in a bear costume. He attempted to join the terrorist group Al-Shabab in July 2010 but was apprehended and questioned at the airport. Shortly thereafter, he was arrested for communicating threats and providing material support to an external terrorist organization. (Bjelopera & Randol, 2010)

A blog post from April 2018 reported that Twitter had blocked over 1.2 million accounts since 2015 due to their involvement in promoting terrorism. The social media platform stated that from July 1, 2017 to December 31, 2017 alone, approximately 275,000 terrorist accounts had been removed. (Siegel & Tucker, 2018)

According to a different article, around 800 accounts that were verified to be supportive of ISIS and other jihadist organizations were suspended. In addition, approximately 18,000 accounts associated with ISIS were identified and banned between the autumn of 2014 and January of 2015. (Charania, 2016)

ISIS is known to conduct highly sophisticated social media campaigns and reportedly earns approximately £3 million daily through illicit activities such as human trafficking, oil smuggling, and theft. The group's targeting strategy is specifically geared towards foreigners. In August of 2014, at the end of Ramadan, ISIS released a 20-minute video featuring footage of Mujahidin. The average age of foreign jihadis is between 18 and 29 years old, and they are predominantly male. Interestingly, women are among the most vocal and visible supporters of ISIS online. One such individual was Aqsa Mehmood, who used Twitter and Tumblr to promote the group's ideology and encourage others to follow her example. (Aly, Macdonald, Jarvis, & Chen, 2016)

Cyber Security System: Pakistan’s Perspective

In March of 2013, The Guardian newspaper reported on information obtained from Edward Snowden's leaked documents, which indicated that the United States' National Security Agency (NSA) had focused significant surveillance efforts on Pakistan, ranking it second only to Iran in terms of targeted countries. (Cassidy, 2013) Subsequently, it was disclosed that the Government Communications Headquarters (GCHQ), the intelligence agency of the United Kingdom, had breached Pakistan's central communications infrastructure by means of hacking. The purpose of this operation was to obtain entry to websites commonly utilized in Pakistan (Tribune, 2015) . As per Microsoft's

reports for the latter half of 2015, Pakistan experienced the greatest incidence of malware attacks, according to their findings. Meanwhile, the Senate Committee on Foreign Affairs of Pakistan revealed that Pakistan was ranked among the leading nations subjected to foreign espionage activities (Rafiq & Rafique, 2013). The current situation in Pakistan with regards to cyber security portrays a vulnerable state, highlighting a deficiency in both policy-making and implementation to combat cyber threats. Hacking, being an illegal and disruptive activity, poses a significant challenge to Pakistan. Since 1998, Indian hackers have targeted the websites of Pakistani government and security agencies, primarily utilizing Denial of Service (DoS) attacks. Records demonstrate that during the period between 1999 and 2008, around 1600 websites in Pakistan were subject to such attacks by Indian hackers (Khan, 2017) . Following its establishment in August 2010, the Indian Cyber Army (ICA), comprising software professionals, became involved in hacking activities with increasing frequency. The group managed to breach nearly 36 websites in Pakistan, including those belonging to the National Accountability Bureau (NAB), Ministry of Foreign Affairs, Ministry of Education, National Database and Registration Authority (NADRA), Ministry of Finance and Pakistan Navy (Shad, 2019). According to a report by a Norwegian cyber security firm in 2013, Indian hackers had been conducting an espionage operation named "Hangover" against Pakistan since 2010. India, being one of the top software-exporting countries worldwide, produces over 100,000 IT professionals annually, giving it an advantage in terms of human expertise and financial resources. This puts India in a position to potentially develop and deploy offensive cyber capabilities against Pakistan. While India has not yet launched a large-scale cyber-attack against Pakistan, cyber skirmishes are becoming increasingly commonplace between the two countries. Such digital assaults tend to occur around significant events, such as Independence Day, and often lead to a tit-for-tat retaliation. Recently, in response to Pakistan's announcement of the death sentence for an Indian spy, Kulbhushan Jadhav, Indian hackers targeted 30 government websites in Pakistan, triggering counter-attacks from Pakistani hackers that were then retaliated by Indian hackers. These incidents indicate the real and significant cybersecurity threats, as the frequency of attacks suggests that it is more than just a minor annoyance.

With the increasing trend of e-government and e-banking, cyber threats are on the rise in Pakistan. The country experiences cases of account hacking, illegal cash withdrawals, and unauthorized or illegal fund transfers almost daily. The cybercrime wing of the Federal Investigation Agency (FIA), the National Response Center for Cyber Crimes (NR3C), received 2,019 complaints in 2017. These complaints can be categorized into three main groups: cases involving harassment, defamation, and blackmailing via social media (76%); cases related to financial fraud (14%); and cases involving threatening calls (5%). The remaining 186 cases were about email hacking, spoofing, etc. It is noteworthy that many cases remain unreported due to the lack of awareness about cyber laws or trust in law enforcement agencies. (kanwal, 2023)

In the aftermath of 9/11, Pakistan was subjected to violent activities such as terrorism, sectarianism, and politico-religious extremism, particularly by sectarian groups and the Tehreek-i-Taliban Pakistan (TTP). Terrorist organizations primarily used physical activities to cause chaos and panic in the country, but have also utilized cyber technology for recruiting members and spreading their propaganda. Following military operations like Zarb-e-Azab against the terrorists and extremist groups, their physical strongholds have been destroyed, leading them to exploit the internet to achieve their sinister goals. The capacity and financial resources of terrorist groups such as Al-Qaeda, ISIS, and TTP to engage in virtual warfare, coupled with alleged backing from hostile security agencies, raise concerns about the potential for such groups to exploit cyberspace. This could enable them to carry out malicious activities and commit cybercrimes such as theft of money.

Conclusion

The need for international cooperation in addressing the challenge of cyber security cannot be overstated. However, the International Telecommunication Union (ITU) has not yet been successful in bringing about a shared understanding among member states for a comprehensive United Nations framework for cyber security. Despite Pakistan's membership in ITU-IMPACT and active participation

in APSIRC-WG, cyber security does not seem to be a top priority on the country's agenda for international trade and agreements. Pakistan's efforts to counter digital terrorism are lacking in effectiveness. While the government introduced the Digital Pakistan Policy in 2017, no specific cyber security system or strategy has been established. Additionally, there is no dedicated agency or department exclusively focused on addressing cyber security concerns in the country. The National Response Center for Cyber Crimes (NR3C) is a unit of FIA tasked with handling cybercrimes, but it faces significant institutional capacity issues, such as insufficient resources and inadequate facilities to effectively combat the malicious activities of hackers.

Recommendations

Cyber technology has brought revolution in our lives. On one hand it is easing our lives but on the other hand radical outfits are exploiting this technology to achieve their goal. They are using online medium with great enthusiasm and vigor. Based on the findings of this study, following are some recommendations to the concerned authorities to counter online radicalization and cyber terrorism:-

- There should be a determined authority to conduct a unified action. Such organization should act as an overarching agency over others.
- Government should engage Islamic scholars to disseminate positivity among people by messaging services. It will help to counter the online radicalization
- T.V. programs should be online to create awareness among the people.
- Initiatives should be taken to regarding Youth development. It will help in building social resiliency against radicalization and terrorism.
- Government should invest more to enhance digital literacy skills.
- Strategy should be made to detect vulnerable groups in the country and make sure their involvement in psycho-social activities.

References

Alava, S., Meigs, D. F., & Hassan, G. (2017). *Youth and violent extremism on social media: Mapping the research.* France: United Nations Educational, Scientific and Cultural Organization.

al-Shishani, M. B. (2010, February 4). Taking al-Qaeda's Jihad to Facebook. *Terrorism Monitor, 8*(5), 3.

Aly, A., Macdonald, S., Jarvis, L., & Chen, T. M. (2016). Terrorist Online Propaganda and Radicalization. *Terrorist Online Propaganda and Radicalization, 40*(1), 1-9.

Bitaab, M., Cho, H., Oest, A., Zhang, P., Sun, Z., Pourmohamad, R., . . . Ahn, G. J. (2020). Scam pandemic: How attackers exploit public fear through phishing. *In 2020 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-10). Boston, MA, USA: IEEE.

Bjelopera, J. P., & Randol, M. A. (2010). *American jihadist terrorism: Combating a Complex Threat.* DIANE Publishing Co.

Cassidy, J. (2013, June 10). *Why Edward Snowden Is a Hero. The New Yorker*

Charania, S. (2016, January 27). Social Media's Potential in Intelligence Collection. *American Intelligence Journal, 33*(2), 94-100.

Chupika, A., & Juneau, T. (2016, November 20). *The Strategies of Cyber Terrorism. Is Cyber Terrorism an effective means to achieving the goals of terrorists.* Ottawa:

Conway, M., & McInerney, L. (2008, December 3-5). Jihadi video and auto-radicalisation: Evidence from an exploratory YouTube study. *Intelligence and Security Informatics , 5376*, 108–118.

Firdous, A. (2018, March). Formulation of Pakistan's Cyber Security Policy: Comparative Approaches. *CISS Insight Journal, 6* (1), 70-94.

Haque, J. (2014, August 3). Analysis: Pakistan's Facebook Dilemma. *Dawn*

Heickero, R. (2014). Cyber Terrorism: Electronic Jihad. *Strategic Analysis*, Vol. 38 (4), p 554-556.

Jaffri, A., Khan, A. H., & Lodhi, N. K. (2023). Hybrid Warfare: New Threats and Complexities for Pakistan. *Pakistan Horizon, 76*(2), 1-16.

kanwal, N. (2023). Analysis of cybercrimes: A Critical Perspective. *International Journal of Computational and Innovative Sciences, 2*(1), 30–39.

Khan, A. (2017, November 24). Cyber Securitization: Need of the Hour for Pakistan. *South Asia*

Khattak, I. (2017, January 19). Pakistan top target for foreign espionage, Senate committee told. *Dawn*

Nawazish, A. M. (2017, May 18). Cyber security: Pakistan's biggest weakness. *The News*

Poduval, S. (2012). Contours of Cyber Security. *Journal of the National Maritime Foundation of India. Maritime Affairs*, 73-94.

Rafiq, A., & Rafique, N. (2013). *Increasing Cyber Threats.* Institute of Strategic Studies Islamabad. Islamabad: Issue Brief.

Rasool, S. (2015, August 12). Cyber security threat in Pakistan: Causes Challenges and Way Forward. *International Scientific Online Journal*, 21 - 34.

SADIA, H. A., Ali, M., & Tariq, N. (2022). Cyber Attacks and Cyber Terrorism: A Weapon and Latest Threat to International Peace and Security. *Research Project*. Islamabad, Pakistan: Department of Law, Bahria University, Islamabad.

Shad, M. R. (2019). Cyber Threat Landscape and Readiness Challenge of Pakistan. *Journal of Strategic Studies, 39*(1).

Siegel, A. A., & Tucker, J. A. (2018, January). The Islamic State's Information Warfare Measuring the Success of ISIS's Online Strategy. *Journal of Language and Politics*, *17*(2), 258 - 280.

Siraj, A. (2018, May 31). Impact of Internet Use on Social Capital: Testing Putnam's Theory of Time Displacement in Urban Pakistan. *The Journal of Social Media in Society, 7*(1), 456-468.

Tribune. (2015, June 23). *British e-spy agency hacked network routers to access almost any internet user in Pakistan. The Express*

Vasilescu, C. (2012). Cyber Attacks:Emerging Threats to the 21st Century Critical Information Infrastructures. *Obrana a strategie (Defence & Strategy)*, 53-62.

Yamin, D. T. (2018). Cyberspace Management in Pakistan. *Governance and Management Review, 3*(1), 46-61.