STM JOURNALS

Journal of
Network Security

https://journals.stmjournals.com/jons

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 12, Issue 3, 2024
September–December
DOI (Journal): 10.37591/JoNS

Research JoNS

Impact of Cyber Security on Modern Warfare

Muhammad Aftab Khalid[1], Ahthasham Sajid[2,*], Fariha Shoukat[3]

Abstract

Cyber technology is frequently utilized to share information and data and to develop communication with a nearly infinite audience. This technology has developed a worldwide network. As a contemporary military instrument, cyber technology has the potential to be used in a variety of ways. Today's cyber warfare dangers might be encountered in a variety of ways since modern cyber warfare has taken a backseat to physical war techniques in the twenty-first century. Extremist groups may also utilize it to spread their religious beliefs. The goal of the dissemination is to generate public support for the terrorist cause and distribute the message. To find and connect with like-minded individuals from across the globe, it is quite inexpensive to use the internet. Additionally, it aids in terrorism-related activities such as fundraising, propaganda, training, and inciting. The ease with which young people can access cyber technology can lead to radicalization in just a few minutes. The potential of cyber technology to promote information and idea sharing—which is acknowledged as a fundamental human right—is just one of its many advantages. To be clear, the same technology may be used to assist terrorism or to incite hatred and violence in society. One problem in the fight against terrorism is the use of cyber technology for radicalization and terrorism.

Keywords: Cyber technology, cyber security, cyberwarfare, terrorism, radicalization, social media

INTRODUCTION

Every aspect of our lives is influenced by the media, from weather predictions to entertainment. Everywhere we go, we are constantly bombarded with media devices, from our mobile phones to digital displays in our homes, businesses, and streets [1]. The media continuously feeds our thoughts, molding, and molding them. Because of this torturous and unknown indoctrination, we are falling prey to our greatest enemy. According to new research, terrorism and the media have been linked in surprising ways. Terrorism feeds the media's need for blood, gore, and other dramatic content, which the media uses to bolster its profits. Unfortunately, terrorists have their sights set precisely on what we have. All that murder and suffering are intended to frighten and intimidate us.

***Author for Correspondence**
Ahthasham Sajid
E-mail: ahthasahm.sajid@riphah.edu.pk

[1]Student, Department of Computer Science, Faculty of ICT, Baluchistan University of Information Technology Engineering and Management Sciences, Quetta, Baluchistan, Pakistan
[2]Assistant Professor, Department of Information Security, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan
[3]Student, Department of Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

Received Date: September 12, 2024
Accepted Date: September 23, 2024
Published Date: October 29, 2024

Citation: Muhammad Aftab Khalid, Ahthasham Sajid, Fariha Shoukat. Impact of Cyber Security on Modern Warfare. Journal of Network Security. 2024; 12(3): 29–33p.

LITERATURE REVIEW

If an act of terrorism is particularly heinous or brutal, it will be widely publicized. Most people turn to the media for information regarding current events and global affairs. The media is a critical tool that influences the general population. When it comes to getting their message out there, the media is an important tool for terrorist organizations. It is interesting to see how they work in harmony [2]. There is general agreement that the Internet serves as a catalyst and enabler of a person's path towards violent political acts rather than being the sole source of radicalization [3]. It is via the media that terrorists can disseminate their message and instill fear among the general population by providing

them with tales that are both emotionally engaging and violent. Terrorists rely on the media to communicate their messages of dread and uncertainty to a far broader audience than immediate victims, and the media plays a critical role in this. As a first step, they seek attention from the public; second, they seek sympathy for their cause; and third, they seek pressure from the public on politicians to do something. The degree of public support that policymakers receive directly correlates with the amount of pressure they face [4]. Terrorists can quickly supply the media with horrifying photos and films, which not only spread their message of dread, but also magnify it considerably through minute-by-minute reporting, re-enacting scenes, and sensationalizing with potent analogies. The government is under pressure to alter its direction and enact new policies and initiatives when citizens worry and respond [5].

In the aftermath of the public uproar following the September 11 attacks in the United States, the government went to war in both Iraq and Afghanistan, but sensationalized and distorted media coverage gave rise to Islamophobia's ugly head. One such instance is this, which not only exacerbates racial and ethnic conflicts within the country but also causes millions of deaths worldwide. There are several ways to deal with this situation. How would the media react if terrorist acts were not publicly covered? As a result, fewer terrorist acts will be carried out, since the terrorists' intended outcomes will be averted. If this is the case, press freedom would be compromised, which might lead to even more unrest if the media came under government control [6]. There are advantages to covering and exposing everything, even if the media is falling into the trap of terrorist organizations. The introduction of censorship is detrimental to democracy and should be avoided at all costs; being informed is always preferable to remaining in the dark. However, the question remains as to how terrorist media coverage may be minimized. People have voiced various viewpoints on the internet. For example, defining terrorism is an important step for the media to take before they can properly distinguish between criminal and terrorist acts [7]. A distorted picture of terrorism has been conjured up by the overuse of the term these days, fueling unwarranted anxiety and dread. Consequently, it inspires other attention seekers to engage in similar actions for non-terrorist reasons. This may be seen in the British press's coverage of the Westminster attack, as well as in previous incidents like it.

Cyberspace as a Lens for Examining Terrorism and Militancy in Pakistan

In Pakistan, cyber technology, fundamentalism, and terrorism are all on the rise, while the corporate media's insatiable drive to capitalize on sensationalism remains its greatest flaw. This can be verified by creating a culture of ethical and responsible media in which reporters understand the impact of their work. Fewer graphics and more educational news pieces are required to break the media's mutually beneficial relationship with radicalism [8]. There is an issue with social media, which is not as easy to control as mainstream media such as TV and newspapers. It is considerably more difficult to censor what people say on social media than in a traditional newspaper because of the speed at which information can be disseminated via such channels. In addition to shutting down accounts that support violence and terrorism, social media sites such as Facebook and Twitter may go a step further by verifying and authenticating posts before they are published. It is believed that peace is not only achieved via negotiations and the official signing of agreements, which is simple for the media to report. A counternarrative against terrorism would be a much more realistic step toward peace for the media. We must decide between fostering terrorism in the media's hungry lap or destroying it in the responsible gaze of society.

CRITICAL ANALYSIS

A Method of Terrorism Involving the Use of Cyber Technology/Modern Warfare

Cyber security is frequently used to victimize the general population and propagate extremist ideology. Propaganda, recruiting, planning, training, and financing are all intertwined in this strategy. Below, we take a closer look at each of these elements.

Propaganda

Terrorists exploit cyber technologies to promote their agendas, which may be rooted in disinformation. Terrorists often use multimedia communication to disseminate their message of justification or explanation for their actions. Different channels and sources exist in cyber security that terrorists use for propaganda. Facebook, Twitter (officially known as X), YouTube, Messenger, Imo, and other Internet-based social media platforms are examples of these sources. Terrorist propaganda often focuses on instilling fear and increasing violence. Many individuals might be affected by the terrorist message being disseminated via cyberspace [9]. To spread their messages, terrorists may only utilize media such as video footage and audio recordings to spread propaganda about terrorism and religious extremism. Fake videos may likewise be seen as genuine on the internet because of the editing and alteration capabilities provided by cyber technology. There is a lack of trust in the state's ability to oversee Internet-based propaganda. They can be readily accessed through the internet, and there are no cyber checks in place for these films. Through propaganda methods, religious sectarian speeches play a critical role in fostering the radicalization and division of society on the internet.

Extremism on the Internet

Online extremism is the process through which individuals, especially young people, come to hold extreme political or religious beliefs after learning about them over the internet. Since the September 11th attacks, the trend of internet polarization has played a critical role in the promotion of religious division and terrorism in Pakistan, particularly among youth. This idea was supported by a vast majority of Pakistani academics and researchers. Extremist religious ideologies are promoted and propagated through polarized sectarian literature created online through violence. Political scientists, academics, and policymakers in Pakistan consistently overlook the issue of internet conversion, which is a growing concern. The Ministry of Information Technology and Telecommunication (MoITT) agreed with this theory.

Questions from the Survey and Responses from the Respondents

1. *Question:* Do you think it is a good idea to give money to religious organizations and support their goals?
   Answer: Giving money to religious groups is deemed reasonable and a good purpose by 80 percent of the people.
2. *Question:* During the hectic market day, where did you receive your religious teachings and media?
   Answer: Sixty percent of Web, Facebook, 20% of WhatsApp, and 10% of religious books were the most common sources of information.
3. *Question:* Do you think it's okay to spread a certain sectarian ideology because you are a member of that splinter group?
   Answer: About 80% of people feel that it is appropriate rather than a religious or anti-Semitic motive.
4. *Question:* Pakistan has been plagued by terrorism, extremism, and religious extremism. Do you believe that cyber technology is to blame?
   Answer: 76% of those polled agree with this statement.

Survey findings concerning internet radicalization and the ideological beliefs of respondents must be considered before delving into the survey results about the political opinions of respondents. To what extent is Islam relevant in today's political landscape, and what role does it play? These concerns have muddled discussions of national identity and unity in the state. The Pakistani people are known for their devotion to Islam, and parliament's precincts must reflect this. In contrast, approximately 52% of those surveyed opposed the state's sectarian nature. In the market, there are two types of financial aid boxes: one for welfare trusts, such as Shokat Khanum and Abdul Star Ahdi One, for religious organizations, such as Tahreeke Labaik Ya Rasool Allah, Dawate Islami, Dawat jihad, Kashmiri cause, and unmarked box [9]. The other is for trust. Money is collected in all Lahore marketplaces based on social welfare

and religious values. The researchers collected data from Lahore's marketplaces to test the theory that internet radicalization is increasing in Pakistan. Market respondents were asked about the type of Facebook posts they had, in addition to their family and friends' photos. Subcategories such as religious, political, economic (business-related), and recreational posts were included in the Facebook post categories, and questions concerning religious posts were asked, presuming that religious harmony is the basis for religious posts.

PREPARATION OF THE RESEARCHER'S REPORT (RECOMMENDATIONS)

Employment

The use of cyber security is not limited to the dissemination of separatist or religious ideology, shielded standpoint in the pattern of posts, publications, or video files, but also aids in the search and recruitment of similar people on a unified system, as well as the sowing of seeds of radicalization through the use of the internet. The employment of propaganda provided via networks such as password-protected websites and limited access to internet chat groups by terrorist organizations as a method of clandestine recruitment is becoming more common. Jobless children and minors, who spend a significant amount of time on the internet, maybe recruited more effectively through cyber technology than any other method available. Because of their exposure to the internet, a large number of schoolchildren and even college students may have become radicalized and sympathetic to terrorist organizations. Terrorist groups use a variety of strategies, such as cartoon characters, short stories, or message-packed video games. The ultimate objective is to instill fear of death in young people and recruit those who, among other things, are fearless when it comes to suicide attacks and death [11]. Owing to advancements in cyber security, terrorist groups can now communicate at a low cost and with a nearly limitless audience. The internet makes it easier for terrorist organizations with a religious bent to communicate with people from all social classes in developing nations such as Pakistan. The internet also facilitates the employment of people who support terrorism and provides scientific support to terrorists working in the nation.

Cyberattacks/Internet Attacks

Cyber threats started as a friendly rivalry between hackers, but with time, they changed into a lucrative game to gain industrial and financial benefits, and ultimately, they turned into a direct threat to the national security of the nation in the issue. The hackers are now referred to as "Key Board Militants," and they act in a certain way to carry out their operations and have specific goals, instruments, and alliances, both state-sponsored and non-state-sponsored. Hacked websites, banks, and information from various military and intelligence organizations in different countries are typical targets for hackers targeting governmental apparatuses. Some governments have even gone so far as to enlist hacking groups and organizations for their national objectives, in addition to breaking into other countries' internet databases. The two methods in which cyber warfare appears are data theft and computer system takeover. The ability to directly operate infrastructures like bridges, war facilities, and other such things is known as system control. Information theft and its destruction are associated with operating system failure. Data theft is the most popular type of cyberterrorism because it poses the least danger to the system control mechanism in use. These cyber terrorists use information and communication technologies (ICTs) for propaganda on websites and social media platforms, as well as for hacking and cyberattacks, to propagate their agendas and messages globally.

Education and Training

There are various ways terrorists might use cyber technology, including films and materials that are backed by their training programs. Today's contemporary soft weapons are made possible by an expanding array of cyber technology, which includes full instructions on how to make various explosive ingredients. For ordinary Muslims in Pakistan, there are a variety of jihad-motivational movies and training programs to help support Afghani and Kashmiri jihad and to oppose the United States and India.

Planning

Additionally, cyber technology allows terrorists to organize covert operations in a safe and secure environment. It is possible to use cyber codes to translate missions into various codes in cyber networks

in the context of cyber technology. According to new United Nations research, terrorists are increasingly using the internet to carry out their acts of violence. 4th Ed, 2012 states "Several criminal law practitioners have claimed that practically every instance of terror convicted involves the use of cyber security" [10]. For example, preparing an act of terrorism often includes distant communication between numerous participants. Terrorists use cyber technology to communicate secretly and attract a wide range of individuals to assist in the planning of terrorist acts. Access to information from several international organizations is also made possible using cyber security.

CONCLUSION

The use of cybersecurity has facilitated online extremism and violence in Pakistan. Globally, separatist extremism is increasing, with Pakistan experiencing a particularly notable increase. Traditional radicalization differs from internet radicalization in Pakistan in terms of the shifting features of these movements. The rate of cyber warfare has swiftly gained traction, complicating already difficult security concerns. As a result, every country must develop a comprehensive strategy to combat cyber security threats for its own sake and that of its citizens. Until the end of This month 2022, according to a MacAfee assessment, 170 million malware performed daily hacking assaults on PCs until the end of this month. Obama also said that cyber warfare is the greatest danger to US security and that they need to employ "Cyber Warriors" to deal with and defeat this threat. A major concern for every country in the world, as seen by the MacAfee study and Obama's remarks, is cyberterrorism. To combat this danger, countries must use non-conventional measures, such as bolstering cyber security. Terrorism in Pakistan is fueled by the proliferation of online radicalization in Pakistani society, facilitated by cyber technology. The federal government should improve cybersecurity measures and keep a close eye on this problem.

REFERENCES

1. Ogun MN. Terrorist use of internet: possible suggestions to prevent the usage for terrorist purposes. J Appl Secur Res. 2012;7:203–17. DOI: 10.1080/19361610.2012.656252.
2. Khan S, Butt KM. Cyber technology, radicalization and terrorism in Pakistan. J Indian Stud. 2017 Dec 31;3(2):119–28.
3. Meleagrou-Hitchens A, Kaderbhai N. Research perspectives on online radicalisation: a literature review, 2006-2016. 2017. Available from: https://icsr.info/wp-content/uploads/2017/05/ICSR-Paper_Research-Perspectives-on-Online-Radicalisation-A-Literature-Review-2006-2016.pdf
4. Whittaker J. Online radicalisation: what we know. 2022. Available from: https://home-affairs.ec.europa.eu/system/files/2023-11/RAN-online-radicalisation_en.pdf
5. Khan RA. Meta-analysis of cyber dominance in modern warfare: attacks and mitigation strategies. Turk J Comput Math Educ (TURCOMAT). 2023 Jul 8;14(3):1051–61.
6. Altmann J, Vidal F, Capurro R, Britz J, Hausmanninger T, Nagenborg M, Nakada M, Weil F. Cyber warfare. Int Rev Inf Ethics. 2013;20:12.
7. Basholli F. Cyber warfare, a new aspect of modern warfare. In: VI International Scientific Conference on Security, CONFSEC 2022 Dec. 2022. p. 52–4.
8. Sheth A, Bhosale S, Kurupkar F. Research paper on cyber security. Emerging advancement and challenges in science, technology and management. Contemporary Research in India [Special Issue]. 2021 Apr 23-24. p. 246.
9. Khan S, Butt KM. Cyber technology, radicalization and terrorism in Pakistan. J Indian Stud. 2017 Dec 31;3(2):119–28.
10. Katyal NK. Criminal law in cyberspace. Univ Pa Law Rev. 2001;149:1003–14. DOI: 10.2307/3312990.
11. Weimann G. Cyber-fatwas and terrorism. Stud Confl Terror. 2011;34:765–81. DOI: 10.1080/1057610X.2011.604831.

