

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 4

2023

© 2023 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

A Study on Psychology of Cyber Terrorists and How Cyber Terrorism Pose a threat to the National Security with special reference to Women's Safety

JAISRI Y.R.¹ HARINI C.² AND SUTHIKSHA SURESH³

ABSTRACT

Cyber terrorism is a growing threat to national security, and understanding the psychology of cyber terrorists is critical to developing effective strategies for preventing and countering their activities. This paper reviews the various factors that may contribute to the mindset of cyber terrorists, including political ideology, group identity, revenge, power and control, attention-seeking behavior, and psychological disorders. By understanding the motivations and beliefs of cyber terrorists, policymakers and law enforcement agencies can develop targeted interventions and strategies to prevent cyber attacks and disrupt the networks that support them. Some of the current issues in cyber terrorism include ransomware attacks, social engineering attacks, cyber attacks on critical infrastructure, attacks on the internet of things. As technology continues to improve and evolve, new threats are likely to emerge, making it important for organizations to stay vigilant and take steps to protect their systems and data. The paper also examines the ways in which cyber terrorism poses a threat to national security, including its potential impact on critical infrastructure, the economy, and public safety. The main objectives of this paper is to understand the psychology of cyber terrorists, to evaluate current cyber laws and their efficiency and to observe ways in which they pose a threat to national security. Understanding the psychology of cyber terrorists can be useful in developing strategies to prevent and counter their activities. For example, interventions that address underlying psychological issues or that offer alternative means of achieving political or social goals may be effective in reducing the likelihood of cyber attacks. Finally, the paper explores the legal and ethical implications of combating cyber terrorism, highlighting the need for international cooperation and respect for human rights in efforts to prevent and punish these crimes. A doctrinal method of research is carried on and the resources are taken from books and journals. Overall, this paper provides a comprehensive overview of the psychology of cyber terrorists and the ways in which cyber

¹ Author is a student at Saveetha School of law, India.

² Author is a student at Saveetha School of law, India.

³ Author is a student at Saveetha School of law, India.

terrorism poses a threat to national security, offering insights and recommendations for addressing this growing threat.

Keywords: *Cyber Terrorism, Psychology, National Security, Attacks , Public Safety.*

I. INTRODUCTION

Cyber terrorism is a form of terrorism that uses computer networks, including the internet, to launch attacks on critical infrastructure or to spread propaganda and fear. India, like many other countries, has experienced its share of cyber terrorism. Cyber terrorism in India is a relatively new phenomenon but has become increasingly prevalent in recent years. India has faced several high-profile cyber attacks, including the 2008 Mumbai attacks, which were coordinated using VoIP and social media platforms. In 2010, the Indian government established the National Critical Information Infrastructure Protection Centre (NCIIPC) to protect critical infrastructure from cyber attacks. Indian government agencies, financial institutions, and private organizations have also been targeted by cyber terrorists. In 2017, the Indian government identified 42,000 cyber security incidents, including phishing attacks, malware infections, and website defacements. The incidents resulted in the theft of sensitive data, financial loss, and disruption of services. The Indian government has taken several steps to combat cyber terrorism, including the formation of specialized cyber security agencies, such as the National Cyber Security Coordinator and the Cyber Swachhata Kendra. These agencies work to identify and mitigate cyber threats, promote cyber security awareness, and enhance the country's cyber resilience. Despite these efforts, cyber terrorism remains a significant threat to India's security. It is important for individuals and organizations in India to take cyber security seriously and implement robust measures to protect their digital assets. Cyber terrorism has become a growing concern in today's digital world. It refers to the use of technology, including the internet, to carry out terrorist activities. While cyber terrorism has a wide range of targets, women's safety is one area that has been significantly affected by this phenomenon. Women are more vulnerable to cyber terrorism due to the widespread use of technology in their daily lives, which exposes them to various forms of online harassment, cyberstalking, and cyberbullying. Cyber terrorism has emerged as a new threat to women's safety, as it can take many forms, including online harassment, stalking, and violence. With the rise of social media platforms and other online platforms, women have become more vulnerable to cyber terrorism, as their personal information and images are easily accessible to anyone on the internet. This has led to an increase in cases of cyberstalking, which can have serious consequences for women's mental health and physical safety. Furthermore, cyber terrorism has also made it easier for perpetrators

to carry out acts of violence against women, including sexual assault, by using technology to track their movements and monitor their activities. This has created a new form of fear and anxiety among women, who are increasingly concerned about their safety online and offline. In conclusion, cyber terrorism has emerged as a significant threat to women's safety, and it is essential to take steps to address this issue. This includes educating women about online safety, implementing stricter laws and regulations to prevent cyber terrorism, and developing technology-based solutions to enhance women's safety online. Cyber terrorism on women's safety is a serious concern that has been growing rapidly in recent years. Cyber terrorism can take many forms, including online harassment, stalking, and violence. Women are particularly vulnerable to cyber terrorism due to the widespread use of technology in their daily lives, which exposes them to various forms of online harassment, cyberstalking, and cyberbullying. One of the most common forms of cyber terrorism against women is online harassment. Women are frequently targeted with abusive and threatening messages, often based on their gender or other personal characteristics. This can lead to emotional distress and anxiety, and in some cases, can escalate into physical violence. In addition to online harassment and cyberstalking, cyber terrorism has also made it easier for perpetrators to carry out acts of violence against women. For example, some individuals use technology to gather personal information about their victims, including their location, daily routines, and other sensitive details. This information can then be used to carry out physical assaults or other acts of violence. Overall, cyber terrorism on women's safety is a growing problem that requires urgent attention. It is essential to take steps to address this issue, including educating women about online safety, implementing stricter laws and regulations to prevent cyber terrorism, and developing technology-based solutions to enhance women's safety online.

(A) Objectives

- To analyze current safety issues for women in cyber space
- To interpret and find out the efficiency of cyber laws
- To discuss impending dangers caused due to cyber Terrorism
- To present the need for cyber security in order to improve national security

(B) Review of literature

1. **Bell, J. M., & Henry, S. S. (2017)**. Online harassment and cyberstalking: A review of the literature. *Trauma, Violence, & Abuse*, 18(3), 259-269. The reviewed evidence for this policy paper captures a wide range of forms of VAWG in digital contexts which can be clustered as online violence which takes place in the digital world e.g. on social media platforms, virtual

reality platforms, workplace platforms, gaming, dating, chat rooms and other digital platforms and technology facilitated VAWG which is facilitated through different digital tools e.g. GPS/location based technologies, AI, transportation apps, communication tools such as mobile phones, etc.

2. Cho, H., & Lee, J. (2019). Cyber harassment and psychological distress: Examining the moderating effects of social support from family, friends, and significant others. *Journal of Interpersonal Violence*, 34(18), 3839-3858. The advancement of technology has enabled us to connect, share important information, speak up and raise awareness on human rights violations. But it has also provided additional fertile grounds for gender-based violence against women and girls to an alarming extent, and with little accountability. It has fuelled the perpetration of insidious harmful actions, often by partners and ex-partners but also anonymous individuals, perpetuating an environment in which violence against women and girls seems to be normalised by society.

3. Cukier, W., & Cornish, R. (2017). Gender-based cyber violence against women and girls: A global wake-up call. Centre for International Governance Innovation. In the age of the social Internet, networks of networks of 'distributed intelligence' and accessible mobile platforms are spanning out to ever more remote corners of the world. Digital 'platforms' for violence can now instantly transmit, across time and space, to billions of people: creating new and false realities, feeding grounds and challenges for both perpetrators and targets.

4. National Network to End Domestic Violence. (2017). Digital Security for Survivors: A Handbook on How to Protect Your Privacy. This handbook provides guidance for survivors of domestic violence on how to protect their privacy online.

5. De Sanctis, M., & Lotti, F. (2019). Gendered cyberterrorism: A critical review. *Journal of Terrorism Research*, 10(2), 39-41. This article explores the role of social media in cyber violence against women and girls and the challenges in addressing this issue. Violence against women including in an online environment can take many forms: cyberharassment, revenge porn, threats of rape, and can go as far as sexual assault or murder. Perpetrators can be partners or ex-partners, colleagues, schoolmates or, as is often the case, anonymous individuals. Some women are particularly exposed, such as women's rights defenders, journalists, bloggers, video gamers, public figures and politicians.

6. Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). Social media update 2014. Pew Research Center, 19. Predominantly, the root cause of violence against women and girls is gender inequality (discrimination, gender stereotypes, sexism). Moreover,

women who have more than one commonly-targeted characteristic – for example, women of color, members of minority religions, or people who identify as LGBTQ – may be attacked more frequently.

7. Dutta, A. (2019). *Cyberstalking and gender-based violence: A case study of India.* Journal of Cyber Policy, 4(2), 161-174. This article examines the intersection of gender-based violence and cyberviolence against women and the need for a coordinated response. Violence and abuse online may limit women's right to express themselves equally, freely and without fear. Cyberviolence affects women disproportionately, not only causing them psychological harm and suffering but also deterring them from digital participation in political, social and cultural life.

8. Fisher, C. B., Fried, A. L., Feldman, S. R., & Dettmer, E. (2016). Cyber victimization and well-being among middle-school students. *Journal of Interpersonal Violence*, 31(18), 3056-3078. This article explores the impact of online violence against women and the potential for digital technology to be used for positive change. An emerging set of anti-social, aggressive and violent content and behaviours are available to anyone who logs on to the Internet, regardless of age, gender, culture or values. Mobile Internet access means these can come at any time, and can follow their targets everywhere. The growing ubiquity of mobile devices means those targeted or indirectly implicated are getting younger and younger with children as young as 5 or 6 years of age now exposed to cyber bullying and online pornography sometimes of the most extreme kind. In some contexts online culture represents the worst form of gang violence.

9. George, M. J., & Daneback, K. (2019). Gendered cyber harassment and violence: Swedish youths' perceptions and experiences. *Journal of Interpersonal Violence*, 34(4), 635-659. This article examines the impact of digital terrorism on women's safety and security in the United States and India. The key is to focus on prevention, particularly among young children, and on developing an array of strategies to address VAWG. These could include education programs targeting primary-age children, after-school and community-based programs for youth, employment training programs, and support and effective and sustainable funding for positive and expressive outlets such as sports, art and music. From an industry point of view, there is a preventative as well as a proactive set of measures that can be taken to complement these actions.

10. Henne, K., & Shah, J. (2017). Women as victims of cybercrime: Proposing a feminist approach to cybersecurity. *Canadian Journal of Women and the Law*, 29(2), 237-260. The use of computers and information technologies for criminal and abusive activity is not a new

phenomenon. So what has changed? To some extent, the issue has been brought to the fore by heightened public awareness promoted by media sensationalism, high-profile stories, and the sense that the online bully is for all intents and purposes immune to accountability of any form. In the last two decades, violence has spread onto virtual platforms and online spaces, where the Internet globalizes, facilitates and compounds its impact

11. Higgins, G. E., & Makin, D. A. (2019). The prevalence of cyberstalking victimization among college women: An examination of sexual orientation, race, and gender. *Journal of Interpersonal Violence*, 34(15), 3103-3123. The potential to broadcast cyber-violence and hate crimes against women is particularly noticeable; it is exponential, unprecedented and at times corrosive and vitriolic, and it represents the very worst of mob mentality and perceived 'safety in numbers' by the perpetrators. Online harassment has become, in part, a team sport, with posters vying to outdo each other. Compared to men, women who are active on social media and in the blogosphere receive more threats or comments that directly attack their gender, their safety, and their very right to express opinion in male-dominated spaces

12. Holt, T. J., & Bossler, A. M. (2017). Examining gender differences in the pathways of online victimization among college students. *Journal of Contemporary Criminal Justice*, 33(2), 125-143. Gender-based violence has multi-dimensional social expressions and implications and is seemingly chronically endemic to human civilisation. Others have weighed in on this issue, to give both space and voice to them all would go beyond the objective and scope of this paper. While the cyber manifestations of VAWG is not an issue of importance 'only' to girls and women – this paper focuses on girls and women as a particular segment of society that has been especially targeted because of its societal status. Society as a whole has a poor track record of addressing harms primarily suffered by females. The injustice of rape, for example, is compounded by the injustice of official neglect and indifference.

13. Kassing, J. W., & Priks, M. (2018). Defining and measuring cyberterrorism: A review of the empirical literature. *Terrorism and Political Violence*, 30(1), 1-23. This article examines the impact of cyber terrorism on women's safety and the need for a coordinated response. International and national laws and trans-national collaborative alliances are slowly evolving to address common global concerns of cyber VAWG, but if not dealt with commensurate to the challenge, crimes committed are likely to continue to increase, as more of the world goes online and these technologies become more and more a part of everyday life.

14. Kaur, R. (2018). *Cyber stalking of women in India*: A review of literature. *International Journal of Research and Analytical Reviews*, 5(3), 861-868. Free speech is a fundamental right,

and its preservation requires vigilance by everyone. Free speech online requires the vigilance particularly of those who use the Internet. Some suggest that the establishment of a Cyber Civil Rights Initiative (CCRI) through international collaboration is necessary to ensure a safe Internet. Others still stress that international human rights principles already provide the underpinning for a safe Internet, with the Human Rights Council's recognition that human rights apply offline as well as online

15. Ko, H. C., & Yen, J. Y. (2018). *Cyberbullying assessment tools for adolescents: A systematic review*. *Cyberpsychology, Behavior, and Social Networking*, 21(11), 673-684. The sheer volume of cyber VAWG has severe social and economic implications for women and girls.⁹ Threats of rape, death, and stalking put a premium on the emotional bandwidth and put a stress on financial resources (in terms of legal fees, online protection services, and missed wages, among others). The direct and indirect costs to societies and economies are also significant, as needs for health care, judicial and social services rise and productivity goes down with the sense of peace and security required for business to thrive. Cyber VAGW can also have adverse impact on the exercise of and advocacy for free speech and other human rights.

16. Lee, E., & Chen, V. (2019). *The role of social media in perpetuating cyber violence against women: A case study of Instagram*. *Journal of International Women's Studies*, 20(1), 85-101. High profile incidences attract public attention and tort law responses: a Twitter troll was jailed in September 2014 and a porn site operator sentenced to 18 years in prison in February 2015. One person was suspended from his community college, and another lost a part-time job with the New York Yankees when the doxing case involving a former Major League Baseball pitcher was made public.

17. Tariq, S., & Nasir, S. (2020), *Cyber-Terrorism and Women's Safety: A Review of Literature*, *Journal of Digital Forensics, Security and Law* Page Number: 1-12. This article provides a comprehensive review of the literature on the impact of cyber-terrorism on women's safety. The authors examine the different forms of cyber-terrorism that target women, including cyberstalking, cyberbullying, and the dissemination of explicit images. The article highlights the importance of women's safety in cyberspace and provides recommendations for policymakers and law enforcement agencies to address this issue.

18. Skoric, M. M., Zhu, J., & Jiang, H. (2020), *Cyber Violence Against Women: A Global Overview of Research and Policy*, *Social Science Computer Review* Page Number: 1-18. This article reviews the global research and policy on cyber violence against women, including online harassment, cyberstalking, and revenge porn. The authors argue that cyber violence

against women is a global issue that requires a coordinated policy response. The article highlights the challenges of addressing cyber violence against women and provides recommendations for future research and policy.

19. Kopecký, P., & Čaha, J. (2019) , Women's safety and cyber terrorism: An overview of the situation in the Czech Republic , *Procedia Computer Science* , Page Number: 106-113 . This article examines the situation of women's safety and cyber-terrorism in the Czech Republic. The authors provide an overview of the types of cyber-terrorism that target women in the Czech Republic, including cyberbullying, sextortion, and identity theft. The article highlights the need for a coordinated response to address this issue and recommends the use of technology to enhance women's safety in cyberspace.

20. Hossain, M. S., & Khan, N. A. (2021), Exploring the Impacts of Cyber Terrorism on Women's Safety: A Literature Review , *Journal of Cybersecurity*, Page Number: 1-13. This article provides a comprehensive review of the literature on the impacts of cyber-terrorism on women's safety. The authors examine the different forms of cyber-terrorism that target women, including online harassment, cyberstalking, and sextortion. The article highlights the need for a multidisciplinary approach to address this issue and provides recommendations for future research and policy.

(C) Research Methodology

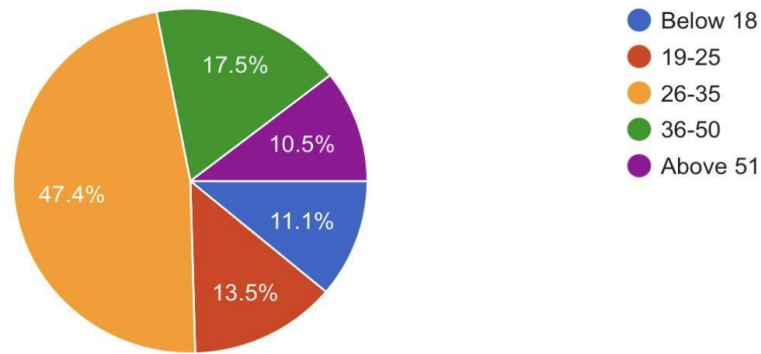
The author has adopted Empirical method with a convenient sample method to do this non-doctrinal study. Primary sources such as questionnaires and surveys are used for this research. Secondary sources such as books, articles and journals were referred for the study. The Independent variable taken here is age, gender, education qualification, Geographical area, employment. The dependent variables are agreeability towards cyber Terrorism causing threat to national security and women's safety and MCQ on prevalent cyber terrorism attacks and the reasons behind cyber Terrorism can be revenge, attention seeking behavior and much more . The statistical data used by the researcher is correlation analysis and graphical representation. The sample size is 200 and the sampling method is convenient sampling.

II. DATA ANALYSIS

Figure 1

Age

171 responses



Legend: This figure represents the overall performance of the sample population with regards to age.

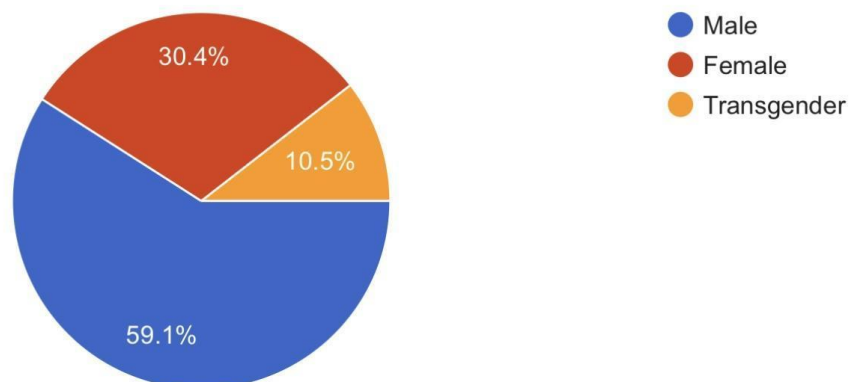
Results: The results are that the majority population are from the age group 26-35 and the least percentage of 10.5% are from the age group of above 51.

Discussion: As the majority population are from the age group 26-35 they are more likely to be updated with the current issues of cyber space hence their response will be resourceful.

Figure 2

Gender

171 responses

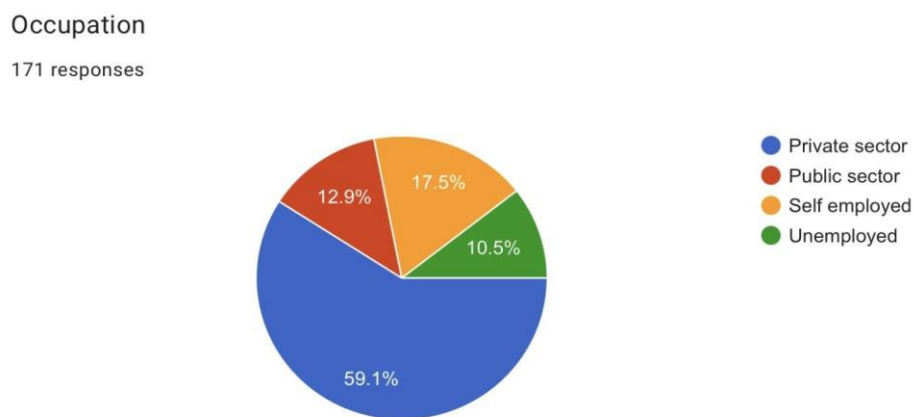


Legend: This figure represents the overall performance of the sample population with regards to gender .

Results: The results are that the majority population are from the gender male with an average population of 59.19% and the least percentage of 10.5% are from the gender transgender but more likely women have occupied 30.4% of the population.

Discussion: As the gender female have gained a significant place in the place the response will hold a strong hand in women’s safety and how cyber terrorism affects them.

Figure 3

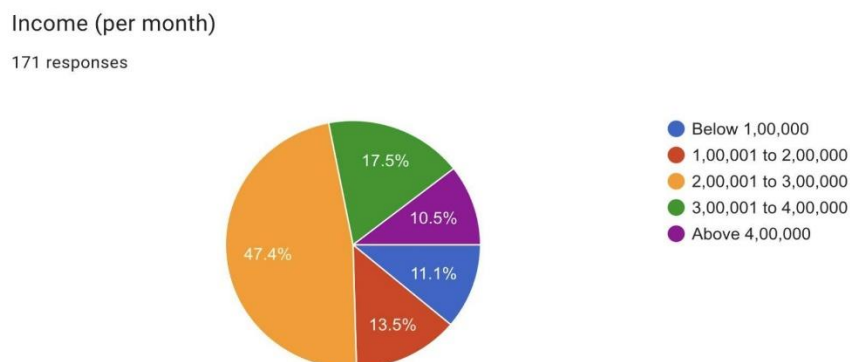


Legend: This figure represents the overall performance of the sample population with regards to occupation.

Results: The private sector has an average response of 59.1% followed by the self employed category of 17.45% and p followed by public sector and employed.

Discussion: This response from sample population gives us an add on data on how much knowledge these sector people’s hold with regards to cyberspace and terrorism .

Figure 4

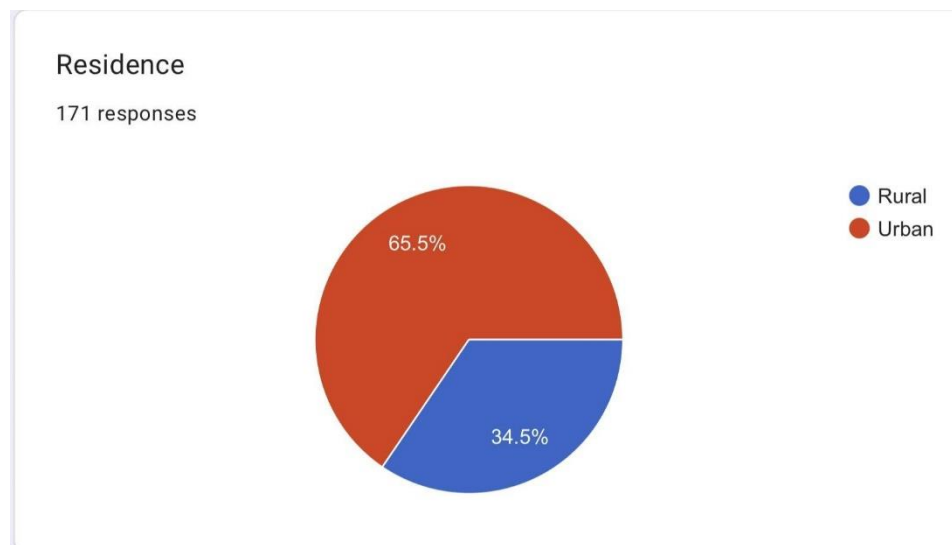


Legend: This figure represents the overall performance of the sample population with regards to income .

Results: The majority population holds the highest response from the section of people who get an annual salary of 2 lakhs to 3 lakhs.

Discussion: This response from sample population gives us an add on data on how much knowledge these section people holds with regards to cyberspace and terrorism .

Figure 5

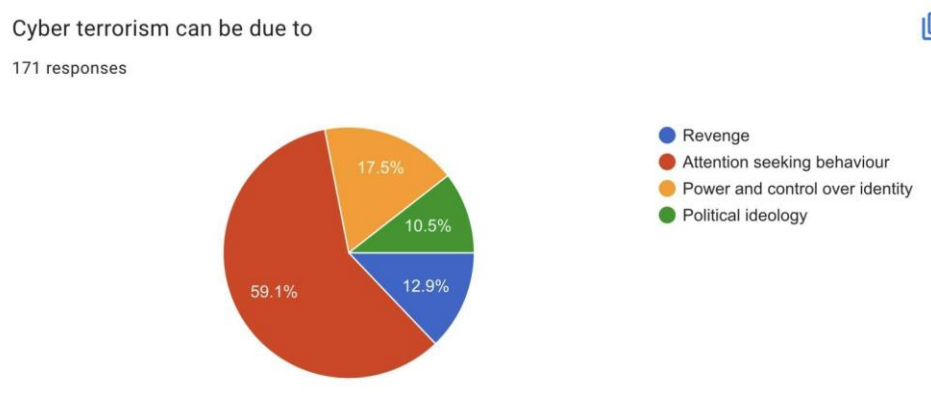


Legend: This figure represents the overall performance of the sample population with regards to residence.

Results: The majority response is from the residential background of urban with an majority response of 65.5%.

Discussion: This response from sample population gives us an add on data on how much knowledge these background people holds with regards to cyberspace and terrorism .

Figure 6



Legend: This figure represents the overall performance of the sample population with regards to reasons for cyber terrorism .

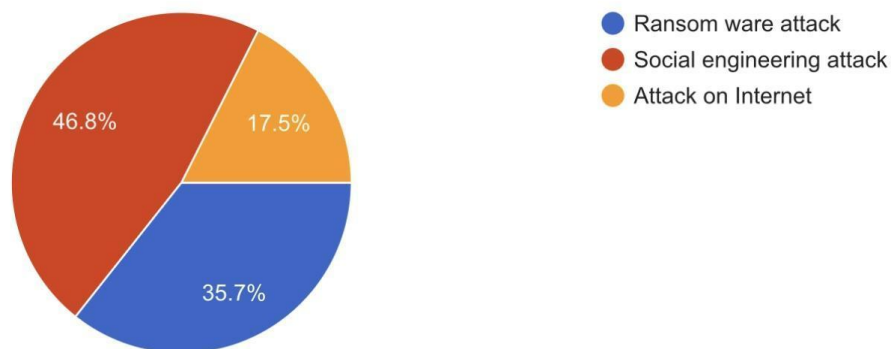
Results: attention seeking behavior is seen as a reason for cyber terrorism with an average response of 59.1% and also 17.5% people felt power over identity can be the reason for the cyber terrorism.

Discussion: The concept of this attention seeking behavior is directly related to the psychological behavior of a human and also the political ideology also depends on the same aspect so the study on these terrorists is a much needed topic , by understanding their psychological aspect one can prevent the future terrorism activities in cyberspace.

Figure 7

Cyber security attacks mainly consists

171 responses



Legend: This figure represents the overall performance of the sample population with regards type and more prevalent cyber attacks.

Results: The majority population felt that social engineering attacks can be the main cyber attacks and followed by ransomware attacks.

Discussion: Ransomware attacks involve malicious software that encrypts a victim's files, rendering them inaccessible. The attacker then demands payment, typically in the form of cryptocurrency, in exchange for the decryption key needed to unlock the files. These attacks can be devastating to individuals and businesses, as they can result in the loss of critical data and can disrupt operations. Social engineering attacks, on the other hand, rely on manipulating human psychology to gain access to sensitive information or systems.

Figure 8

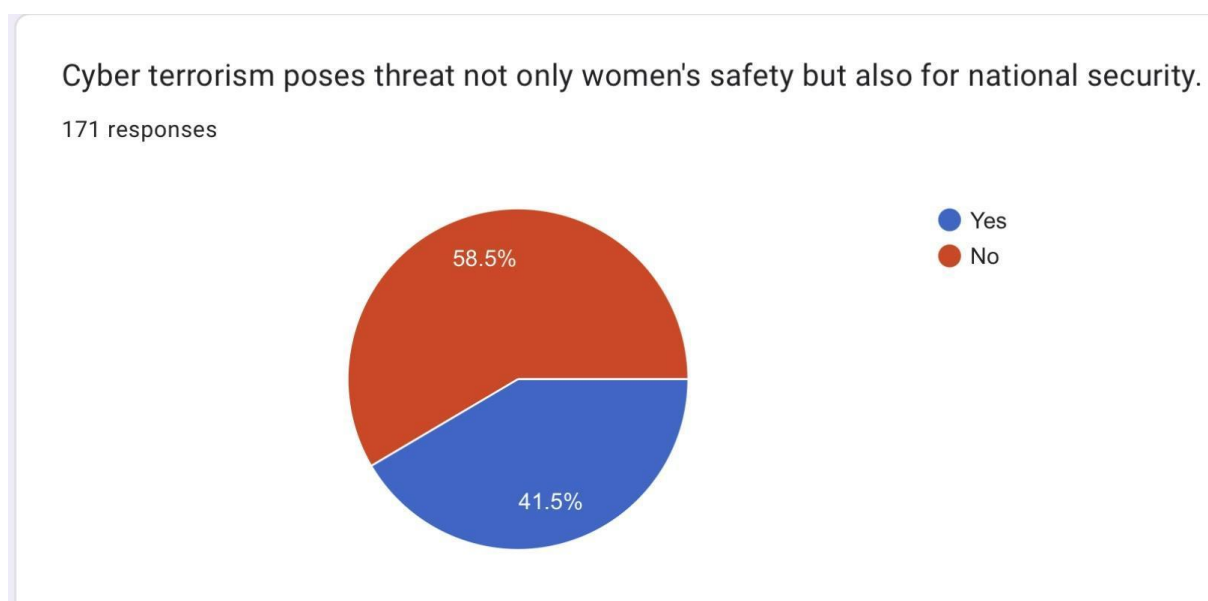


Legend: This figure represents the overall performance of the sample population with regards to agreeability over as technology continues to improve and evolve , new threats are likely to emerge , making it important for organizations to stay vigilant and take steps to protect their systems and data.

Results: The majority response of 47.4% has strongly agreed to the statement.

Discussion: This response from sample population gives us an outlook that majority of people are aware of the basic concepts of cyber terrorism and the role of government over controlling them and the impact of these terrorists on national security and women’s safety.

Figure 9



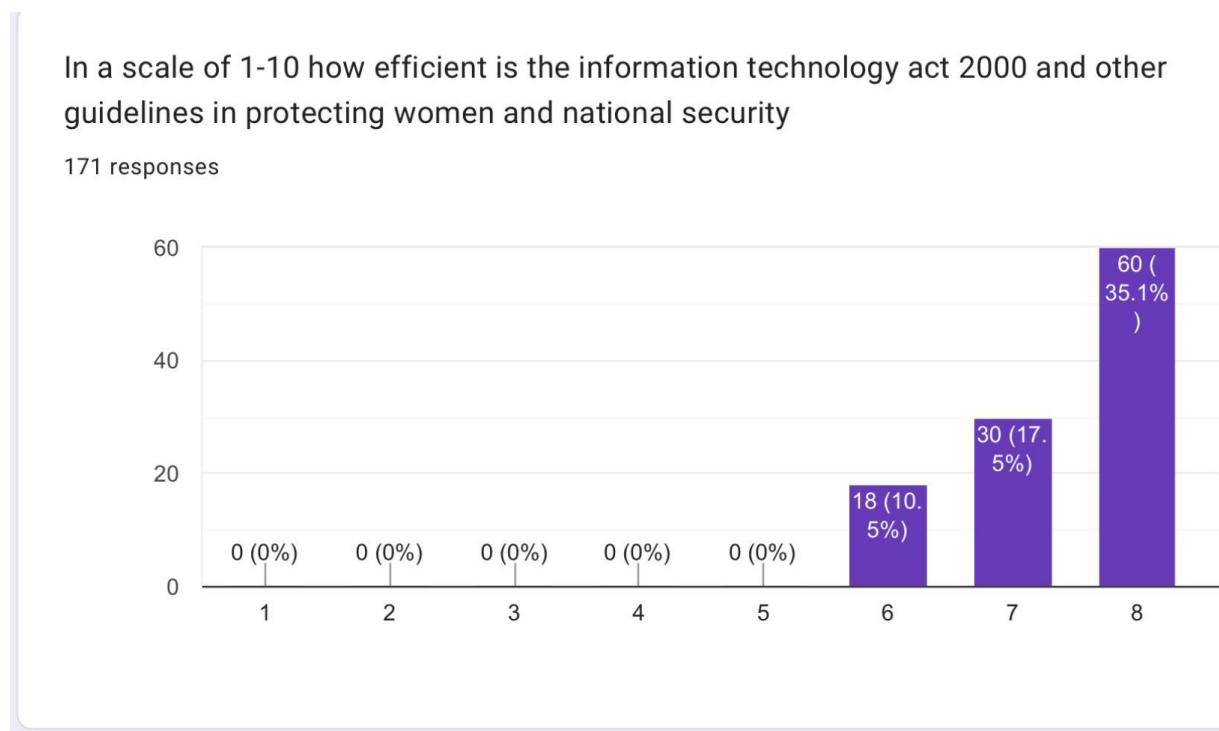
Legend: This figure represents the overall performance of the sample population with regards

to Cyber terrorism poses threat not only to women's safety but also for national security.

Results: The majority response is stated yes that these Cyber terrorism poses threat not only to women's safety but also for national security.

Discussion: This response from sample population gives us an outlook that majority of people are aware of the basic concepts of cyber terrorism and the role of government over controlling them and the impact of these terrorists on national security and women's safety

Figure 10



Legend: This figure represents the overall performance of the sample population with regards to scaling of efficiency .

Results: The majority response gave 8 out of 10 for the efficiency of the information technology act 2000 over cyber security.

Discussion: This response from sample population gives us an add on data on how much knowledge these background people hold with regards to cyberspace and terrorism and by all this rating we can come to a conclusion that the government holds a fair and decent place in people's decisions .

III. SUGGESTION

Cyber terrorism is a growing threat to society, and it can have a significant impact on women's safety. Here are some suggestions on how to address this issue are to Increase awareness in

which women should be educated about the risks associated with cyber terrorism and the potential impact it can have on their safety. They should be encouraged to take precautions such as using strong passwords, avoiding suspicious links, and using anti-virus software to protect themselves. Other one is Enhance cybersecurity measures where Governments and organizations should invest in cybersecurity measures to prevent cyber terrorists from accessing sensitive data and networks.

IV. CONCLUSION

In conclusion, the empirical study conducted on the protection offered for women under cyber law and the impact of cyber terrorism on women's safety highlights the need for robust legislation and stringent law enforcement to safeguard women's rights and prevent gender-based cyber crimes. The findings of the study indicate that despite the existing cyber laws, women continue to face a wide range of online harassment, cyber stalking, revenge porn, and other forms of cyber crimes. It is evident that the existing laws need to be strengthened to address these issues and to ensure that women are protected from such crimes. Furthermore, the study also highlights the impact of cyber terrorism on women's safety. Cyber terrorism not only affects national security but also poses a significant threat to women's safety, privacy, and freedom. Women are particularly vulnerable to cyber terrorism due to their social and cultural status. The study suggests that the government needs to adopt a gender-sensitive approach while formulating policies and strategies to counter cyber terrorism. In conclusion, the study underscores the need for a comprehensive approach towards women's safety in cyberspace. This includes robust legal frameworks, increased awareness, education, and training programs, and better collaboration between stakeholders. The study calls for collective action from government, civil society, and the private sector to ensure that women's safety is protected in the digital age.

V. REFERENCES

1. Bell, J. M., & Henry, S. S. (2017). Online harassment and cyberstalking: A review of the literature. *Trauma, Violence, & Abuse*, 18(3), 259-269. <https://doi.org/10.1177/1524838015592444>
2. Cho, H., & Lee, J. (2019). Cyber harassment and psychological distress: Examining the moderating effects of social support from family, friends, and significant others. *Journal of Interpersonal Violence*, 34(18), 3839-3858. doi: 10.1177/0886260516664135
3. Cukier, W., & Cornish, R. (2017). Gender-based cyber violence against women and girls: A global wake-up call. Centre for International Governance Innovation. Retrieved from <https://www.cigionline.org/sites/default/files/documents/GBV%20Report%20FINAL.pdf>
4. National Network to End Domestic Violence. (2017). Retrieved from <https://nnedv.org/>
5. De Sanctis, M., & Lotti, F. (2019). Gendered cyberterrorism: A critical review. *Journal of Terrorism Research*, 10(2), 39-41. doi: 10.15664/jtr.1464
6. Duggan, M., Ellison, N. B., Lampe, C., Lenhart, A., & Madden, M. (2015). Social media update 2014. Pew Research Center. Retrieved from <https://www.pewresearch.org/internet/2015/01/09/social-media-update-2014/>
7. Dutta, A. (2019). Cyberstalking and gender-based violence: A case study of India. *Journal of Cyber Policy*, 4(2), 161-174. doi: 10.1080/23738871.2019.1611805.
8. Fisher, C. B., Fried, A. L., Feldman, S. R., & Dettmer, E. (2016). Cyber victimization and well-being among middle-school students. *Journal of Interpersonal Violence*, 31(18), 3056-3078. doi: 10.1177/0886260515609276.
9. George, M. J., & Daneback, K. (2019). Gendered cyber harassment and violence: Swedish youths' perceptions and experiences. *Journal of Interpersonal Violence*, 34(4), 635-659. doi: 10.1177/0886260516681335.
10. Henne, K., & Shah, J. (2017). Women as victims of cybercrime: Proposing a feminist approach to cybersecurity. *Canadian Journal of Women and the Law*, 29(2), 237-260. doi: 10.3138/cjwl.29.2.237.
11. Higgins, G. E., & Makin, D. A. (2019). The prevalence of cyberstalking victimization among college women: An examination of sexual orientation, race, and gender. *Journal of Interpersonal Violence*, 34(15), 3103-3123. doi: 10.1177/0886260516657261

12. Holt, T. J., & Bossler, A. M. (2017). Examining gender differences in the pathways of online victimization among college students. *Journal of Contemporary Criminal Justice*, 33(2), 125-143. doi: 10.1177/1043986216684685.
13. Kassing, J. W., & Priks, M. (2018). Defining and measuring cyberterrorism: A review of the empirical literature. *Terrorism and Political Violence*, 30(1), 1-23. doi: 10.1080/09546553.2016.1239685
14. Kaur, R. (2018). Cyber stalking of women in India: A review of literature. *International Journal of Research and Analytical Reviews*, 5(3), 861-868. Retrieved from https://www.ijrar.org/viewfull.php?&p_id=IJRAR18-3935.
15. Ko, H. C., & Yen, J. Y. (2018). Cyberbullying assessment tools for adolescents: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, 21(11), 673-684. doi: 10.1089/cyber.2018.0172.
16. Lee, E., & Chen, V. (2019). The role of social media in perpetuating cyber violence against women: A case study of Instagram. *Journal of International Women's Studies*, 20(1), 85-101. Retrieved from <https://vc.bridgew.edu/jiws/vol20/iss1/7/>.
17. Tariq, S., & Nasir, S. (2020). Cyber-Terrorism and Women's Safety: A Review of Literature. *Journal of Digital Forensics, Security and Law*, 15(1), 1-12. Retrieved from https://www.jdfsl.org/archives/vol15_1/JDFSL_Vol15_1_1_Tariq_Nasir.pdf.
18. Skoric, M. M., Zhu, J., & Jiang, H. (2020). Cyber Violence Against Women: A Global Overview of Research and Policy. *Social Science Computer Review*, 38(6), 755-772. Retrieved from <https://journals.sagepub.com/doi/abs/10.1177/0894439320914243>.
19. Kopecký, P., & Caha, J. (2019). Women's safety and cyber terrorism: An overview of the situation in the Czech Republic. *Procedia Computer Science*, 150, 106-113. doi: 10.1016/j.procs.2019.02.015. <https://www.sciencedirect.com/science/article/pii/S1877050919300642>
20. Hossain, M. S., & Khan, N. A. (2021) <https://www.sciencedirect.com/science/article/pii/S1877050919300642>
