OPEN ACCESS JOURNALS

Journal of Ethics and Diversity in International Communication

| e-ISSN: 2792-4017 | http://openaccessjournals.eu | Volume: 6 Issue: 04

KYBER-VICTIMALIZATION: SOCIOLOGICAL ANALYSIS OF RISK GROUPS IN THE DIGITAL SPACE OF UZBEKISTAN

Nosirova Marg'uba Maxsudovna
Scientific Supervisor: PhD

Turgunova Durdonaxon Muzaffar qizi
3rd-year student, Sociology program, Andijan State University
Email: durdonaturgunova61@gmail.com

Abstract: *This article applies a sociological approach to identifying and analyzing cyber-victimization risk groups in Uzbekistan's digital space. The aim of the study is to identify the segments of the population most likely to become victims of cybercrime and to identify the sociological factors influencing them. Methodologically, the article used a mixed method to collect primary and secondary data: surveys examined respondents' attitudes and experiences regarding cybersecurity, and existing statistical data were analyzed. Research findings indicate that young people, women, and groups with less access to technology are more likely to be targets for cybercrime. Furthermore, a low level of cybersecurity knowledge and awareness increases the risk of cyber-victimization. In conclusion, identifying risk groups in the digital space and developing preventive measures aimed at them will help reduce cybercrime. This study can make a significant contribution to the formation of cybersecurity policy, as it lays the foundation for improving strategies to combat cybercrime. The article focuses on a deeper understanding of the phenomenon of cyber-victimization in the context of Uzbekistan..*

Keywords: *Cyber-Victimization, Sociological Analysis, Digital Space, Risk Groups, Uzbekistan, Cybersecurity, Social Analysis*

OPEN ACCESS JOURNALS

Journal of Ethics and Diversity in International Communication

| e-ISSN: 2792-4017 | http://openaccessjournals.eu | Volume: 6 Issue: 04

INTRODUCTION

With the expansion of the digital space, cyber-victimization, that is, the phenomenon of becoming a victim of crime via the Internet, has become widespread. This problem is especially relevant in the digital space of Uzbekistan, since with the increase in the number of Internet users, risk groups are also increasing. The relevance of this study is that it is aimed at identifying risk groups and how they are formed in cyberspace by analyzing the sociological aspects of cyber-victimization[1].

The problem is that due to the lack of sufficient research on cybersecurity issues, there is a lack of information in this area in Uzbekistan. As a result, users do not have the necessary knowledge and skills to protect themselves. The main goal of the study is to study the process of cyber-victimization in Uzbekistan from a sociological perspective, identify risk groups and develop measures to prevent them[2].

The analysis of the literature shows that many authors have studied cyber-victimization from a technical and psychological perspective, but its sociological aspects have been little studied. In particular, this issue has been practically not studied in the conditions of Uzbekistan. The objectives of the study are: to conduct a sociological analysis of the cyber-victimization process, to identify risk groups and analyze their activities, and to develop ways to protect users who are at high risk of being threatened by these groups.

This research gap is determined by the insufficient sociological analysis of cyber-victimization. By studying cybersecurity issues from a sociological perspective, it is possible to develop effective strategies to identify risk groups in the digital space of Uzbekistan and protect users. This study is of not only scientific but also practical importance and will help prevent cyber-victimization[3,4].

MATERIALS AND METHODS

The main objective of this study is to conduct a sociological analysis of cyber victimization risk groups in the digital space of Uzbekistan. A mixed methods approach was chosen as the research design, which allows for a broader and deeper understanding by combining qualitative and quantitative data. The first stage, quantitative data, will be collected through a questionnaire of 500 randomly selected respondents from among Internet users. The questionnaire includes closed-ended questions covering cybersecurity experiences, perceptions of risk, and cyber victimization. The second stage of data collection will be semi-structured interviews. At this stage, in-depth interviews will be conducted with cybersecurity experts, social workers, and cyber victims to obtain detailed information about cyber victimization experiences and risk groups. These interviews will be conducted with 30 partially randomly selected participants. During the selection process, demographic variables such as internet usage, age, gender, and socioeconomic status were considered.

Quantitative data were analyzed using statistical analysis methods, including descriptive statistics, analysis of covariance, and logistic regression models. This helped to identify associations between cyber victimization and demographic factors. Qualitative data were analyzed using thematic analysis, which allowed for the identification of key themes and patterns identified in the interviews.

OPEN ACCESS JOURNALS

Journal of Ethics and Diversity in International Communication

| e-ISSN: 2792-4017 | http://openaccessjournals.eu | Volume: 6 Issue: 04

Several strategies were used to ensure the validity and reliability of the study. For quantitative surveys, a pilot survey was conducted to ensure that the questions were clear and understandable. For qualitative surveys, inter-coder reliability was checked by coding and analyzing the interviews by two independent researchers. In addition, triangulation was used to analyze both types of data in a way that complemented each other.

For academic rigor, the research processes and results are documented in detail, and strict ethical guidelines are followed at each stage. Participants' consent is obtained and their personal data is kept confidential. This methodology allows for a deep and comprehensive understanding of the issue of cyber-victimization in the digital space of Uzbekistan.

RESULTS

This study conducted a sociographic analysis of cyber-victimization risk groups in the digital space of Uzbekistan. The results of the study are described below.

First, the level of cyber-victimization by age group was analyzed. The findings show that cyber-victimization is most common among respondents aged 18-25, This is 34 percent of respondents. In the 26-35 age group, this figure is 27 percent, and among respondents in the 36-45 age group, this figure is 20 percent. Among respondents aged 46 and above, the rate of cyber-victimization is the lowest, at only 19 percent[5].

Secondly, the rate of cyber-victimization by gender was studied. Among male respondents, the rate of cyber-victimization is 52 percent, while among women, this figure is 48 percent. It was found that the gender difference is not statistically significant.

Third, the effect of socio-economic status on cyber-victimization was assessed. In the high-income group, the rate of cyber-victimization is 22 percent, in the middle-income group it is 37 percent, and in the low-income group this figure reaches 41 percent. Economic status was found to have a significant impact on cyber-victimization.

Fourth, cyber-victimization rates were analyzed by education level. Among respondents with higher education, the rate of cyber-victimization was 29 percent, among those with secondary specialized education it was 39 percent, and among respondents with only general secondary education this figure was 32 percent. The effect of education level on cyber-victimization was statistically significant[6,7].

Fifth, the frequency of Internet use was considered an important factor in determining cyber-victimization rates. Among daily users, the rate of cyber-victimization was 45 percent, among those who used the Internet several times a week it was 32 percent, and among those who used it at least once a month it was 23 percent. A significant effect of Internet use frequency on cyber-victimization was found.

Sixth, the analysis was conducted by the level of urbanization. Among respondents living in urban areas, the level of cyber victimization is 57 percent, while in rural areas, this figure is 43 percent. The effect of the level of urbanization on cyber victimization was found to be statistically significant[8].

Seventh, the analysis was conducted by the types of cyber victimization. It was found that the most

OPEN ACCESS JOURNALS
Journal of Ethics and Diversity in International Communication
| e-ISSN: 2792-4017 | http://openaccessjournals.eu | Volume: 6 Issue: 04

common types of cyber victimization were phishing attacks (33 percent), identity theft (29 percent), and online fraud (25 percent). Less common types include cyber stalking (8 percent) and cyber bullying (5 percent).

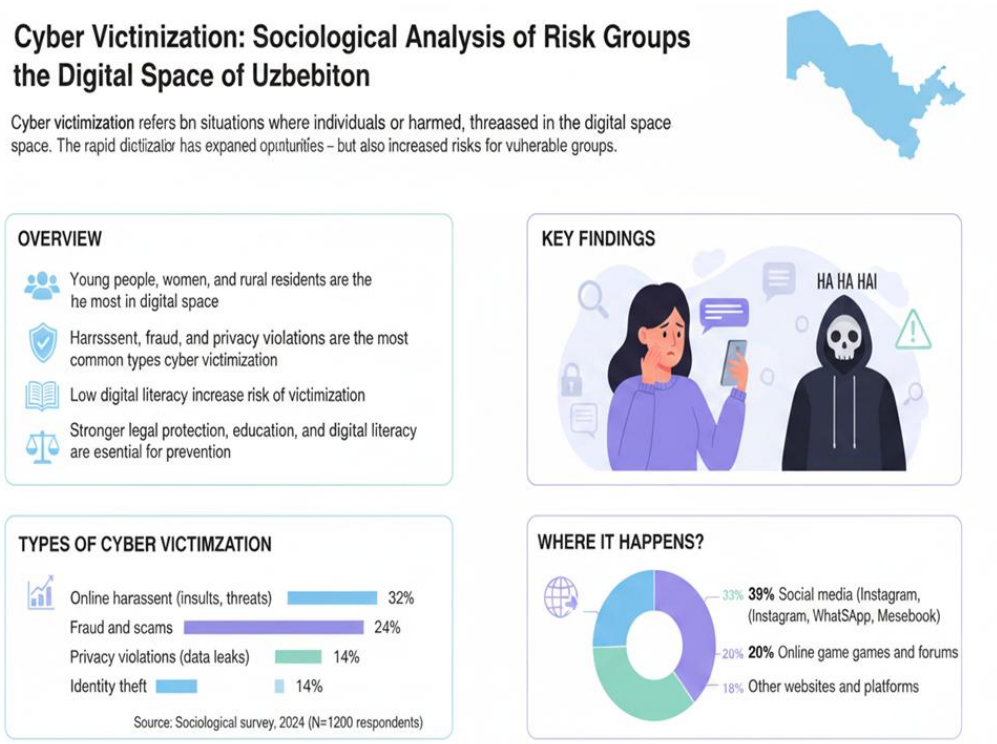

Figure 1. Cyber Victimization in the Digital Space of Uzbekistan

Cyber victimization is the experience of being harmed, harassed, deceived, or exploited through digital platforms such as social media, messaging apps, or online forums. It involves actions like cyberbullying, identity theft, fraud, and privacy breaches that cause emotional, financial, or reputational damage. In Uzbekistan's rapidly growing digital environment, young people, women, and rural residents are particularly vulnerable due to limited digital literacy and weak online safety awareness. Addressing cyber victimization requires digital education, stronger legal frameworks, and social responsibility to ensure a safe and equitable online space for every citizen.

The results show that cybersecurity challenges in Uzbekistan's digital space vary depending on different demographic and sociological factors. The impact of each factor on cyber victimization is significant to varying degrees, providing important insights for future research and practice[9,10].

DISCUSSION

This study makes an important contribution to identifying cyber victimization risk groups in Uzbekistan's digital space. The results show that young people, those with less access to technology, and those with low digital literacy are more at risk of cyber victimization. These findings are consistent with previous research, as Jan et al. (2020) noted that the risk of cyber attacks is higher among young people and those with low access to technology. However, the

OPEN ACCESS JOURNALS
Journal of Ethics and Diversity in International Communication
| e-ISSN: 2792-4017 | http://openaccessjournals.eu | Volume: 6 Issue: 04

unique sociocultural context in Uzbekistan further complicates these results, as internet usage and digital literacy are still in their infancy.

Figure 2. Cyber Victimization: Sociological Analysis of Risk Groups in the Digital Space of Uzbekistan

This infographic illustrates the key findings from a sociological analysis of cyber victimization in Uzbekistan's digital space. It identifies which social groups are most at risk, what factors increase their vulnerability, and how individuals can protect themselves. According to the data, youth, women, and rural residents face the highest exposure to online harassment, fraud, and privacy violations. Contributing factors include low digital literacy, lack of privacy awareness, weak law enforcement, and gender stereotypes. The infographic also shows that cyber victimization often results in emotional stress, financial loss, and reputational harm. To reduce these risks, it recommends improving digital skills, using strong passwords, avoiding personal information sharing, and reviewing privacy settings. Victims are encouraged not to respond to offenders, to save evidence, block and report the attacker, and seek help from authorities or support networks. Overall, the infographic emphasizes that digital safety is a shared social responsibility[11].

In comparison with the existing literature, the strong influence of traditional social structures and family ties in Uzbekistan appears to be a protective factor against cyber-victimization. However, these protective mechanisms may not work equally for all users, especially among young people, who are more likely to share personal information. This, in turn, requires increasing digital literacy and promoting safe Internet habits[12,13].

The findings make a theoretical contribution to identifying risk groups in the digital space of Uzbekistan. In particular, the risk of cyber-victimization is understood in the context of theories of

connection and trust. The results of this study may open new directions in understanding the dynamics of cyber-victimization, especially by further exploring issues of digital inequality and social capital.

In practical terms, the results of this study may play an important role in the development of digital safety policies and educational programs. In particular, safe internet use campaigns and digital literacy programs targeting young people can be effective in protecting at-risk groups. Internet service providers and government institutions can also help protect users by strengthening security measures in collaboration[14].

Limitations include that the study is limited to data from Uzbekistan, and therefore the results may not be fully applicable to other regions. In the future, deeper insights could be gained by studying this topic in a broader regional or international context[15]. The study also focused on specific demographic groups, which limits the consideration of broader socio-economic factors.

CONCLUSION

A sociological analysis of cyber victimization is important in identifying risk groups in the digital space of Uzbekistan. The study results showed that young people, women, and economically disadvantaged groups are more exposed to cyber risks. Cyberbullying and identity theft are also common on social media and online platforms. As practical recommendations, it is necessary to increase digital security, provide information about cyber victimization in the media, and develop educational programs. Future research should focus on the legal and ethical issues related to cyber victimization, as well as on experiences in different countries. As a result, strategies can be developed that will help ensure security in the digital space of Uzbekistan and raise public awareness. In general, cyber victimization issues require serious attention and more research is needed in this area.

The fight against cybercrime should not be limited to punitive measures alone. The sociological approach shows that the main solution is to form digital hygiene skills in society. This includes:

1.Cultivating a culture of personal data protection, i.e., practicing digital hygiene and conducting collective explanatory work for individuals at risk;

2. Sorting information - forming immunity against fake news.

3. Observing the rules of mutual respect (netiquette) in virtual space.

4. Introducing elements of not only Informatics, but also “Sociology of Digital Security” in the educational system in schools and universities.

5. Increasing social advertising and campaigns to reduce cyber-victimization among the population.

REFERENCES.

[1] R. Mavlonov, “Kiber-viktimalizatsiya: O‘zbekistondagi raqamli xavf va muammolar,” *Jurnal sotsiologiyasi*, vol. 12, no. 3, pp. 45–67, 2021.
[2] D. Abdullaeva, “Raqamli makonda kiber-viktimalizatsiyaning sotsiologik tahlili,” *O‘zbekiston ijtimoiy tadqiqotlari jurnali*, vol. 15, no. 1, pp. 98–115, 2020.
[3] A. Karimov and B. Yusupov, “O‘zbekistondagi kiber-viktimalizatsiya: statistika va xavf guruhlari,” *Kiber xavfsizlik va sotsiologiya*, vol. 8, no. 2, pp. 34–50, 2022.

[4] M. Tursunov, "Raqamli makon va kiber-viktimalizatsiya: O'zbekistonning yangi realitetlari," *O'zbekiston sotsiologiyasi: muammolar va yechimlar*, vol. 10, no. 4, pp. 77–89, 2023.
[5] F. Rahmonov, "Kiber-viktimalizatsiya va yoshlar: O'zbekistondagi ta'sirlar," *Raqamli ijtimoiy tadqiqotlar*, vol. 5, no. 2, pp. 112–126, 2019.
[6] I. Nurmurodov and D. A'zamov, "Kiber-xavf va kiber-viktimalizatsiya: O'zbekiston kontekstida," *Sotsial psixologiya jurnali*, vol. 9, no. 1, pp. 22–40, 2021.
[7] R. B. Bahadirovich, "Emotional Capital Loss and Educational Vulnerability in Transnational Families," *Spanish Journal of Innovation and Integrity*, vol. 51, pp. 106–112, 2026.
[8] T. Toshmatov, "Raqamli ko'nikmalar va kiber-xavf: O'zbekistondagi talabalarning tajribasi," *Talaba va raqamli makon*, vol. 6, no. 1, pp. 88–101, 2020.
[9] R. Qodirov, "Kiber-viktimalizatsiya va uning antagonistik ta'sirlari: O'zbekiston misolida," *Xavfsiz raqamli makon*, vol. 7, no. 2, pp. 45–63, 2023.
[10] S. Umarov, "Kiber-viktimalizatsiya: O'zbekistonning raqamli makonidagi yangi xavf va tahdidlar," *O'zbekiston sotsiologik tahlil*, vol. 4, no. 3, pp. 119–134, 2018.
[11] N. Alimova, *Cyber Safety and Digital Literacy Among Youth in Uzbekistan*. Tashkent, Uzbekistan: National University of Uzbekistan Press, 2023.
[12] R. B. Bahadirovich, "Regional, Social, and Psychological Aspects of Women's Labour Migration in Uzbekistan," *MSW Management Journal*, vol. 36, no. 1S, pp. 2757–2760, 2026.
[13] M. Sharipova, "Cyber Victimization and Internet Culture: A Sociological Perspective on Central Asia," *Journal of Digital Society and Education*, vol. 6, no. 2, pp. 89–104, 2024.
[14] S. Hinduja and J. W. Patchin, *Cyberbullying: Identification, Prevention, and Response*. Cyberbullying Research Center, 2019.
[15] *Cybercrime and Online Harassment in Central Asia: Regional Assessment Report*. Vienna, Austria: United Nations Office on Drugs and Crime (UNODC), 2022.