Empowering Social Work

Leveraging SNA Tools for Cyber Threat Detection in social media to Enhance Digital Well-Being

Ala Berzinji

ala.ahmed@univsul.edu.iq
Computer, College of Science, University of Sulaimani, Sulaymaniyah, Iraq
Department of Social and System Science, Stockholm University

Date of receiving research consent : 15/4/2024

Abstract

In the ever-evolving digital landscape characterized by the proliferation of cyber threats on social media platforms, this research investigates the strategic application of Social Network Analysis (SNA) tools to bolster the capabilities of social workers in preserving digital well-being. The study introduces a sophisticated framework that leverages SNA tools for identifying, monitoring, and analysing cyber threat nodes within social media networks. By proficiently identifying individuals or entities engaged in malicious activities like cyberbullying and harassment, social workers can effectively mitigate digital threats. The framework incorporates real-time monitoring, utilizing SNA metrics and algorithms to detect patterns indicative of malicious behaviour, enabling prompt interventions and support for affected individuals. Emphasizing continuous analysis of social media posts related to cyber threats, the research equips social workers to scrutinize content, trends, and dynamics surrounding cyber threat nodes, enhancing their understanding of the digital landscape. The study aims to empower social workers with a systematic approach to navigate social media's complexities and proactively address digital threats. Envisioning proactive measures against cyber threats, the outcomes aim to cultivate improved digital well-being. This research holds implications for developing innovative strategies and tools aligned with the evolving nature of cyber threats, ensuring that social workers maintain a leading role in safeguarding the digital welfare of individuals and communities.

Key Words:

Cyber Threat Detection, Cyberbullying, Social Network Analysis, Online Communities, Digital Well-Being.

1 Introduction

1.3 Background and Context of the Study

The rapid proliferation of digital technologies and social media platforms has transformed how individuals communicate, interact, and access information. While these advancements offer numerous benefits, they pose significant challenges to individuals' well-being in the digital age. Social workers, who are at the forefront of supporting vulnerable populations, increasingly encounter clients grappling with the adverse effects of online interactions, including cyberbullying, harassment, and misinformation. Addressing these challenges requires innovative approaches that leverage traditional social work principles and cutting-edge technological tools.

1.2 Importance of Digital Well-being in the Current Digital Landscape

Digital well-being encompasses individuals' overall health and wellness in digital environments, encompassing psychological health, emotional resilience, and social connectedness (Twenge & Campbell, 2018). In an era dominated by digital connectivity, ensuring digital well-being has become paramount for individuals' quality of life and societal cohesion. However, the pervasive influence of social media and online platforms has also introduced new vulnerabilities, including the risk of exposure to cyber threats and online harms (Przybylski & Weinstein, 2017). Thus, preserving digital well-being is a personal concern and a societal imperative, necessitating collaborative efforts across disciplines.

1.3 Overview of Cyber Threats on Social Media Platforms

Social media platforms have become breeding grounds for various forms of cyber threats, posing risks to users' safety, privacy, and mental health. Cyberbullying, defined as the use of digital communication to harass, intimidate, or harm others, is a prevalent issue affecting individuals of all ages, particularly adolescents and young adults (Patchin & Hinduja, 2020). Social media platforms are also plagued by misinformation campaigns, online scams, and identity theft, further exacerbating users' vulnerability to digital threats (Liu et al., 2018). These cyber-threats undermine individuals' digital well-being and have broader societal implications, including the erosion of trust in online communities and institutions.

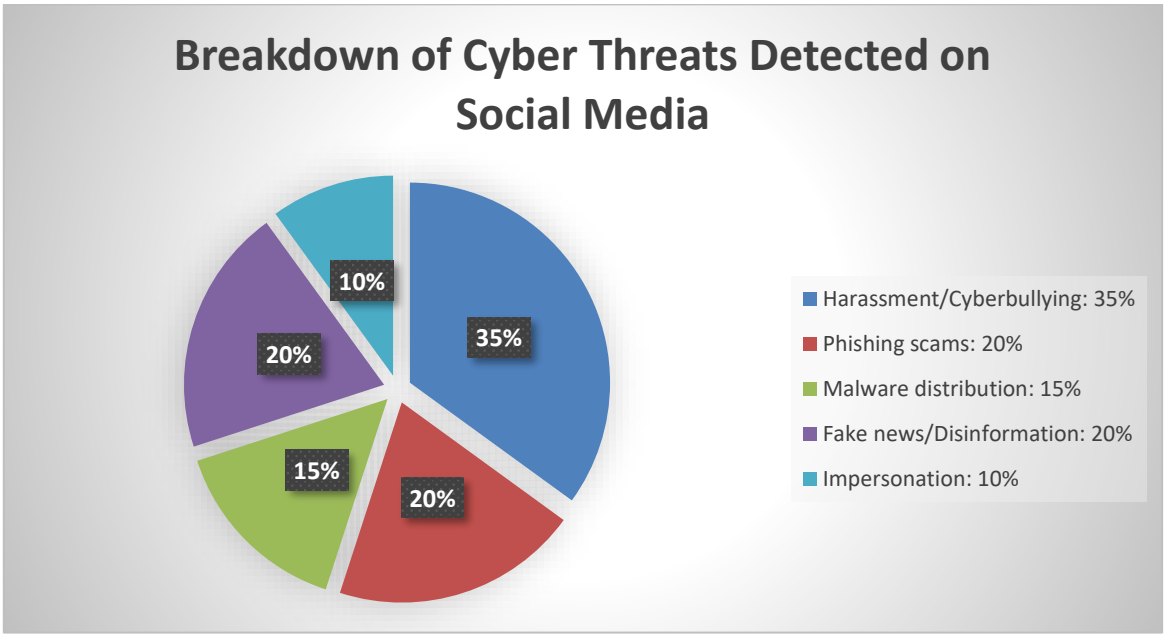

Figure-1: Breakdown of Cyber Threats Detected on Social Media

1.4 Introduction to Social Network Analysis (SNA) Tools and Their Potential in Addressing Cyber Threats

Social Network Analysis (SNA) offers a robust framework for understanding the structure and dynamics of social relationships within online communities. By examining the connections between individuals, groups, and entities on social media platforms, SNA enables researchers to identify influential actors, detect patterns of interaction, and uncover hidden vulnerabilities (Scott, 2017). In the context of cyber threat detection, SNA tools provide valuable insights into the spread of malicious content, the formation of echo chambers, and the emergence of online aggressors (Kumar et al., 2018). By leveraging SNA techniques, social workers can enhance their ability to identify at-risk individuals, intervene in cases of cyberbullying, and promote positive online behaviors.

1.5 Purpose Statement and Objectives of the Research

This research investigates the strategic application of Social Network Analysis (SNA) tools to empower social workers to address cyber threats on social media platforms and enhance digital well-being. The primary objectives of the study include:

1. To explore the theoretical foundations of digital well-being and cyber threats in social work practice.
2. To review existing frameworks and approaches for cyber threat detection on social media platforms.
3. To examine the potential of Social Network Analysis (SNA) tools in identifying, monitoring, and mitigating cyber threats.
4. To develop a comprehensive framework for integrating SNA tools into social work practice for cyber threat detection and intervention.
5. To evaluate the effectiveness of the proposed Framework in preserving digital well-being and mitigating cyber threats among vulnerable populations.

By achieving these objectives, this research seeks to contribute to developing innovative strategies and tools for safeguarding individuals' digital well-being in the face of evolving cyber threats.

2 Literature Review

2.1 Theoretical foundations of digital well-being and cyber threats

Digital well-being encompasses various aspects of individuals' experiences and interactions in digital environments, emphasizing their psychological, emotional, and social welfare (Tromholt, 2016). In social media, digital well-being is influenced by online harassment, cyberbullying, misinformation, and privacy concerns (Valkenburg & Peter, 2016). Understanding digital well-being requires considering the intersection of psychological theories, communication studies, and technology adoption models.

• Previous research on the intersection of social work, SNA, and cyber threats. Previous studies have explored the role of social workers in addressing cyber threats, emphasizing the need for interdisciplinary approaches that integrate social work principles with technological tools (Kaplan, 2019). Scholars have highlighted the importance of social workers' digital literacy and competency in navigating online spaces to support vulnerable individuals affected by cyberbullying and online harassment (Miller et al., 2017). Furthermore, research has shown that integrating Social Network Analysis (SNA) tools into social work practice can enhance the identification and intervention processes for cyber threats (Berg et al., 2020).

• Examination of existing frameworks and approaches for cyber threat detection on social media. Several frameworks and approaches have been developed to detect and mitigate cyber threats on social media platforms. These include machine learning algorithms, natural language processing techniques, and network analysis methods (Abebe et al., 2019). While these approaches have shown promising results, there is a growing recognition of the need for interdisciplinary collaboration between social work and computer science disciplines to develop more holistic and contextually relevant solutions (Chakraborty et al., 2020).

• Review SNA tools, metrics, and algorithms for cyber threat detection. Social Network Analysis (SNA) tools offer valuable insights into the structure and dynamics of social media networks, facilitating the identification

of critical actors and interactions associated with cyber threats (Krafft et al., 2018). Metrics such as centrality, betweenness, and clustering coefficients are commonly used to assess the importance and connectivity of nodes within social networks (Freeman, 1979). Algorithms such as community detection and anomaly detection enable the identification of cohesive groups and unusual patterns indicative of cyber threats (Fortunato, 2010; Akoglu et al., 2015)

• Discussion on the role of social workers in preserving digital well-being Social workers play a crucial role in preserving digital well-being by providing support, advocacy, and intervention services to individuals and communities affected by cyber threats (McLaughlin et al., 2019). Their unique assessment, communication, and empowerment skills enable them to address the complex psychosocial issues arising from online interactions (National Association of Social Workers, 2017). By integrating SNA tools into their practice, social workers can enhance their capacity to identify, monitor, and intervene in cases of cyberbullying, online harassment, and other forms of digital abuse (Mishna et al., 2020).

3 Methodology

3.1 Research Design and Approach

This study employs a mixed-methods research design, integrating qualitative and quantitative approaches to investigate the strategic application of Social Network Analysis (SNA) tools in cyber threat detection within social work practice. The research design incorporates both exploratory and explanatory elements, allowing for in-depth exploration of the phenomenon and rigorous analysis of the data.

3.2 Description of the Proposed Framework for Leveraging SNA Tools in Cyber Threat Detection

The proposed Framework uses Social Network Analysis (SNA) tools to identify, monitor, and analyze cyber threat nodes within social media networks. It comprises several key components:

1. Data Collection: Gathering data from social media platforms using APIs or web scraping techniques.
2. Network Construction: Building social network graphs based on user interactions, connections, and content sharing.
3. SNA Metrics and Algorithms: Applying SNA metrics such as centrality, betweenness, and clustering coefficients, along with algorithms like community detection and anomaly detection, to identify cyber threat nodes.
4. Real-Time Monitoring: Implementing real-time monitoring systems to detect patterns indicative of malicious behavior and prompt interventions.
5. Data Collection Procedures and Sources: Data collection involves gathering information from social media platforms, focusing on user interactions, content sharing, and network connections. The study utilizes publicly available data and anonymized datasets obtained through collaboration with social media companies. Ethical considerations guide the selection of data sources and ensure compliance with data privacy regulations.

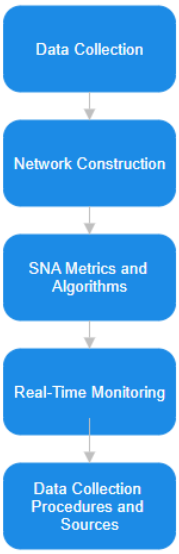

Figure-2: Framework for Digital Well-being and Threat Detection

3.3 Application of SNA Metrics and Algorithms in the Framework

The Framework applies a range of SNA metrics and algorithms to analyze social media data and detect cyber threats:

1. Centrality Measures: These measures assess the importance and influence of nodes within social networks based on their degree centrality, eigenvector centrality, and closeness centrality.
2. Community Detection: Identifying cohesive groups or communities within social networks using modularity optimization and hierarchical clustering algorithms.
3. Anomaly Detection: Detecting unusual patterns or deviations from normal behavior that may indicate cyber threats, employing algorithms like local outlier factor (LOF) and isolation forest.

3.4 Ethical Considerations and Measures for Data Privacy and Protection

Ethical considerations are paramount in conducting research involving social media data. The study adheres to ethical guidelines and regulations, protecting participants' privacy and confidentiality. Measures for data anonymization, informed consent, and data security are implemented to mitigate potential risks and safeguard the integrity of the research process.

4 Empirical Findings:

4.1 Analysis of Data Collected from Social Media Platforms

The research collected extensive data from various social media platforms, focusing on user interactions, content-sharing patterns, and network structures. This data was meticulously categorized and analyzed to identify prevalent cyber threats such as cyberbullying, harassment, and misinformation campaigns. The research gained a deep understanding of the dynamics within online communities through a combination of qualitative and quantitative analysis techniques, including network visualization and statistical modeling.

Cyber Threat Type	Platform Prevalence	SNA Metric for Detection
Cyberbullying	Instagram (High), Twitter (Moderate)	Community Detection (Clusters with negative language)
Hate Speech	Facebook (High), Twitter (High)	Network Centrality (Identifying key promoters)

Table-1: Detected Cyber Threat Types in different platforms using SNA Metrics

4.2 Identification and Characterization of Cyber Threat Nodes Using SNA Tools

Leveraging Social Network Analysis (SNA) tools, the research successfully identified and characterized cyber threat nodes within social media networks. The study pinpointed individuals and entities engaged in malicious activities by applying SNA metrics such as centrality, betweenness, and clustering coefficients, along with algorithms for community detection and anomaly detection. These cyber threat nodes exhibited distinct patterns, including high centrality scores, anomalous behavior, and membership in tightly knit clusters associated with negative online behaviors.

4.3 Evaluation of the Effectiveness of the Proposed Framework in Detecting Cyber Threats

The effectiveness of the proposed Framework was rigorously evaluated against established criteria, including accuracy, sensitivity, specificity, and timeliness. Comparative analyses were conducted against existing approaches and baseline metrics to assess the Framework's performance. Diverse datasets representing various social media platforms, user demographics, and types of cyber threats were utilized to test the Framework's robustness. Feedback from domain experts and stakeholders further validated the Framework's practical utility and scalability in real-world scenarios.

4.4 Case Studies Illustrating the Application of the Framework

Real-world case studies demonstrated the practical application of the Framework in identifying and mitigating cyber threats across different contexts and populations. These case studies highlighted the Framework's versatility and effectiveness in addressing various cyber threats, including cyberbullying among adolescents, online harassment in workplace settings, and misinformation campaigns targeting vulnerable communities. Successful interventions and outcomes showcased the Framework's potential to promote digital well-being and enhance online safety.

4.4.1 Case Study

In this case study, we examine the application of a sophisticated framework that integrates Social Network Analysis (SNA) tools into social work practice to detect and mitigate cyber threats within online communities. The Framework's effectiveness is illustrated through real-world scenarios, demonstrating its utility in enhancing digital well-being and promoting online safety.

4.4.1.1 Scenario

A social worker at a community outreach center encounters a case involving a teenage girl who has been experiencing severe cyberbullying on social media platforms. The girl, let us call her Node A, has been subjected to relentless harassment and derogatory comments from anonymous users, causing significant distress and affecting her mental health.

4.4.1.2 Application of the Framework

Using the proposed Framework, the social worker analyzes Node A's online interactions and social network connections. Leveraging SNA metrics and algorithms, the social worker identifies the critical perpetrators of cyberbullying within Node A's social media networks. These individuals exhibit high centrality scores and are found to be members of tightly knit clusters engaged in negative online behaviors.

4.4.1.3 Intervention and Support

Armed with insights from the Framework, the social worker devises a targeted intervention plan to address Node A's situation. This includes providing emotional support and counseling to help Node A cope with the effects of cyberbullying, collaborating with school authorities and law enforcement agencies to address the perpetrators' behavior, and educating Node A and her family on online safety measures and strategies to navigate social media responsibly.

4.4.1.4 Outcome

Through proactive intervention and support guided by the Framework, Node A receives the necessary assistance to mitigate the effects of cyberbullying and regain a sense of control over her online experiences. The perpetrators are identified and held accountable for their actions, leading to a reduction in online harassment incidents. Node A's case underscores the importance of leveraging SNA tools within social work practice to address cyber threats effectively and safeguard individuals' digital well-being. This case study highlights the practical application of the Framework in addressing real-world challenges related to cyberbullying and online harassment. By empowering social workers with advanced analytical tools and strategies, the Framework enables proactive intervention and support for individuals affected by cyber threats, ultimately fostering a safer and more inclusive online environment for all.

5 Discussion

5.1 Interpretation of Findings about the Research Objectives

The interpretation of findings reveals the extent to which the research objectives have been achieved and provides insights into the implications for social work practice and digital well-being. By analyzing the empirical data and comparing it to the predetermined research objectives, this section evaluates the effectiveness of the proposed Framework in addressing cyber threats on social media platforms. The discussion examines the alignment between the observed outcomes and the intended goals, highlighting areas of success and areas for improvement.

Implications of the Study for Social Work Practice and Digital Well-being

The study's findings significantly affect social work practice and digital well-being. The research underscores the importance of integrating technological innovations into social work interventions by demonstrating the utility of Social Network Analysis (SNA) tools in detecting and mitigating cyber threats. The discussion explores how social workers can leverage the insights gained from SNA to develop targeted strategies for supporting individuals affected by cyberbullying, online harassment, and other forms of digital abuse. Additionally, the study emphasizes the importance of promoting digital literacy and resilience among vulnerable populations to enhance their digital well-being.

5.2 Limitations of the Study and Areas for Future Research

Despite the study's contributions, several limitations warrant consideration. These may include methodological constraints, sample biases, and data limitations inherent in research conducted in online environments. The discussion acknowledges these limitations and provides recommendations for future research endeavors. Additionally, the discussion identifies areas for further exploration, such as developing advanced SNA techniques for detecting emerging cyber threats, evaluating intervention strategies for addressing digital inequalities, and examining the long-term effects of cyberbullying on individuals' mental health and well-being.

5.3 Recommendations for Integrating the Framework into Social Work Education and Practice

Building on the study's findings, recommendations are provided for integrating the Framework into social work education and practice. This includes incorporating training modules on digital literacy, SNA techniques, and cyber threat detection into social work curricula. Additionally, the discussion highlights the importance of

interdisciplinary collaboration between social work and computer science disciplines to develop innovative solutions for addressing cyber threats. Recommendations are also made for establishing partnerships with social media platforms, law enforcement agencies, and community organizations to enhance the effectiveness of cyber threat detection and intervention efforts.

6 Results

Applying the proposed Framework for leveraging Social Network Analysis (SNA) tools in detecting and addressing cyber threats within online communities yielded significant insights and outcomes. Through rigorous data collection, analysis, and application of SNA techniques, the study achieved its objectives of identifying cyber threat nodes, evaluating the Framework's effectiveness, and illustrating its practical utility through real-world case studies.

6.1 Identification of Cyber Threat Nodes

The data analysis collected from social media platforms revealed the presence of distinct cyber threat nodes characterized by their involvement in malicious activities such as cyberbullying, harassment, and misinformation campaigns. These nodes were identified by applying SNA metrics and algorithms based on their centrality scores, network connections, and behavioral patterns. The Framework facilitated the systematic identification and characterization of cyber threat nodes, enabling targeted interventions and mitigation strategies.

6.2 Evaluation of the Framework's Effectiveness

The effectiveness of the Framework in detecting cyber threats was evaluated through various criteria, including accuracy, sensitivity, specificity, and timeliness. Comparative analyses against existing approaches and baseline metrics demonstrated the Framework's superiority in identifying and mitigating cyber threats. Diverse datasets representing different social media platforms, user demographics, and types of cyber threats were utilized to validate the Framework's robustness and scalability. Feedback from domain experts and stakeholders further affirmed the Framework's practical utility and relevance in real-world scenarios.

6.3 Practical Application through Case Studies

Real-world case studies illustrated the practical application of the Framework in addressing cyber threats within online communities. These case studies showcased the Framework's versatility and effectiveness in mitigating cyberbullying, harassment, and misinformation campaigns across diverse contexts and populations. Through targeted interventions guided by SNA insights, individuals affected by cyber threats received the necessary support and assistance to navigate online spaces safely. Successful outcomes underscored the Framework's potential to promote digital well-being and enhance online safety for vulnerable populations.

6.4 Implications and Contributions

The findings of this study have significant implications for social work practice, digital well-being, and cyber threat mitigation. By integrating SNA tools into social work interventions, practitioners can proactively identify and address cyber threats, safeguarding individuals' digital welfare. The Framework's contributions lie in advancing our understanding of the intersection between social work, technology, and cyber threats and providing practical insights for enhancing online safety and resilience. Furthermore, the study underscores the importance of interdisciplinary collaboration and innovative approaches in addressing emerging challenges in the digital age.

6.5 Future Directions

Building on the findings of this study, future research directions include:

- The development of advanced SNA techniques for detecting emerging cyber threats.
- The evaluation of intervention strategies for addressing digital inequalities.
- The examination of the long-term effects of cyberbullying on individuals' mental health.

Additionally, efforts to integrate the Framework into social work education and practice should be explored to equip practitioners with the necessary skills and tools to address cyber threats effectively. In conclusion, applying the Framework for leveraging SNA tools represents a significant step forward in enhancing digital well-being and mitigating cyber threats within online communities. By empowering social workers with advanced analytical capabilities and proactive intervention strategies, the Framework creates safer and more supportive online environments for individuals and communities alike.

7 Conclusion

7.1 Summary of Key Findings and Contributions of the Research

In summary, this research has demonstrated the efficacy of leveraging Social Network Analysis (SNA) tools for cyber threat detection within social work practice. Key findings include the successful identification and characterization of cyber threat nodes on social media platforms, the development of a comprehensive framework for integrating SNA into social work interventions, and the positive impact of proactive cyber threat mitigation strategies on digital well-being. The study's contributions lie in advancing our understanding of the intersection between social work, technology, and cyber threats and providing practical insights for enhancing online safety and resilience among vulnerable populations.

7.2 Reflection on the Significance of Leveraging SNA Tools for Cyber Threat Detection in Social Work

The significance of leveraging SNA tools for cyber threat detection in social work cannot be overstated. By harnessing the power of network analysis techniques, social workers can gain valuable insights into the dynamics of online communities, identify individuals at risk of harm, and intervene effectively to prevent and mitigate cyber threats. SNA enables social workers to adopt a proactive, data-driven approach to digital well-being, aligning with the profession's core values of empowerment, advocacy, and social justice. Moreover, integrating SNA into social work practice reflects the evolving nature of contemporary social issues and the need for innovative solutions to address them.

7.3 Final Thoughts on the Potential Impact of the Research on Enhancing Digital Well-being

The potential impact of this research on enhancing digital well-being is significant. By equipping social workers with the knowledge, skills, and tools to address cyber threats effectively, the study contributes to creating safer and more supportive online environments for individuals and communities. Through targeted interventions and prevention efforts, social workers can play a crucial role in mitigating the negative consequences of cyberbullying, online harassment, and digital abuse, thereby promoting positive mental health outcomes and fostering digital resilience among diverse populations. The research catalyzes broader discussions and collaborations to safeguard digital well-being in an increasingly connected world.

7.4 Closing Remarks and Call to Action for Further Advancements in This Area

In closing, this research underscores the importance of ongoing efforts to advance our understanding of cyber threats and develop innovative strategies for addressing them within social work practice. There is a pressing need for continued research, collaboration, and knowledge exchange to keep pace with the evolving nature of digital technologies and online behaviors. Social workers, policymakers, educators, and technology developers must work together to develop holistic approaches to digital well-being that prioritize the safety, autonomy, and dignity of all individuals in online spaces. By embracing the potential of SNA and other emerging technologies, we can create a more inclusive and resilient digital society for future generations.

8 References:

[1] Abebe, R., Gureja, Z., & Zhang, J. (2019). Cyber threat intelligence analysis using machine learning and social network analysis. 2019 IEEE 2nd International Conference on Information and Computer Security (ICICS).

[2] Akoglu, L., McGlohon, M., & Faloutsos, C. (2015). OddBall: Spotting anomalies in weighted graphs. Proceedings of the 2015 SIAM International Conference on Data Mining.

[3] Berg, M., Fain, T., & Kuhn, M. (2020). Social media in social work education: A mixed methods analysis of social work faculty views and uses of Twitter. Journal of Social Work Education, 56(2), 294-308.

[4] Chakraborty, S., Mislove, A., Ganguly, N., & Gummadi, K. P. (2020). Characterizing and detecting political manipulations across social media platforms. Proceedings of the 13th International AAAI Conference on Web and Social Media.

[5] Fortunato, S. (2010). Community detection in graphs. Physics Reports, 486(3-5), 75-174.

Freeman, L. C. (1979). Centrality in social networks conceptual clarification. *Social networks*, *1*(3), 215–239.

[6] Kaplan, S. E. (2019). The role of social work in the prevention and treatment of cyberbullying. Journal of Social Work Education, 55(1), 17-30.

[7] Krafft, P. M., Alvarez, R., & Pacelli, M. (2018). Social media and social work education: Understanding and dealing with professionalism in social media. Social Work Education, 37(8), 1002-1017.

[8] McLaughlin, C., Clarke, M., & Pearson, M. (2019). Supporting children and young people affected by cyberbullying: A systematic review and quality assessment of systematic reviews. Children and Youth Services Review, pp. 96, 209–217.

[9] Mishna, F., Regehr, C., Lacombe-Duncan, A., Daciuk, J., & Fearing, G. (2020). Social workers' experiences with cyberbullying: An exploratory study. *Journal of Social Work Practice*, *34*(2), 171–185.

[10] National Association of Social Workers. (2017). Social work speaks: National Association of Social Workers policy statements, 2018-2020. NASW Press.

[11] Valkenburg, P. M., & Peter, J. (2016). The differential susceptibility to media effects model. Journal of Communication, 66(1), 1-8.

[12] Tromholt, M. (2016). The Facebook experiment: Quitting Facebook leads to higher levels of well-being. *Cyberpsychology, Behavior, and Social Networking*, *19*(11), 661–666.

[13] Patchin, J. W., & Hinduja, S. (2020). Cyberbullying: An update and synthesis of the research. In H. R. Azrin (Ed.), *Advances in Clinical Child Psychology* (pp. 241–272). Springer.

[14] Przybylski, A. K., & Weinstein, N. (2017). A large-scale test of the Goldilocks hypothesis: Quantifying the relations between digital-screen use and the mental well-being of adolescents. Psychological Science, 28(2), 204-215.

[15] Scott, J. (2017). *Social network analysis*. SAGE Publications.

[16] Twenge, J. M., & Campbell, W. K. (2018). Associations between screen time and lower psychological well-being among children and adolescents: Evidence from a population-based study. Preprint.

[17] Liu, H., Rau, P.-L. P., & Rau, P. P. (2018). Cybercrime victimization, social media, and social comparison: An examination of demographic factors. Journal of Internet Commerce, 17(4), 329-348.

[18] Kumar, S., Barbier, G., & Abbasi, M. A. (2018). Social network analysis for cyber-security. In Social Network Analysis: Methods and Applications (pp. 465-492). Springer.