Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.1.00402

RESEARCH ARTICLE

Prevention of Cyberbullying in Online Games: Intervention of Cybersecurity Strategies

Muhammad Fakhru Rizuan Che Omar[1*], Noor Aziah Abdullah[2], Mohd. Nizam Saad[3]

[1,2,3]School of Multimedia Technology and Communication, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia.

ARTICLE INFO

Received: Apr 24, 2024

Accepted: Jul 18, 2024

Keywords

Cyberbullying Behavior

Online Games

Cybersecurity strategies

Theory Planned Behavior

Conceptual Framework

***Corresponding Author:**

fakhru.rizuan@gmail.com

ABSTRACT

Cyberbullying occurs in online games, and it is a major concern in the gaming community. However, there are no specific guidelines for preventing cyberbullying in online games following cybersecurity strategies. This paper aims to determine specified preventions in cyber security strategies in Malaysia for TPB to combat cyberbullying in online games. The purposive sampling technique was employed. Four informants (a Game Developer, a Counsellor, a Cybersecurity Expert, and an Academician) were selected for semi-structured interviews. Thematic analysis for the interview was employed. All experts suggested pillars 2 and 4 in Cybersecurity Strategies 2020-2024: strengthening legislative framework and enforcement and enhancing national cyber security capacity and capability building as essential preventions that TPB can adapt to combat cyberbullying in online games. By applying the findings of this research, policymakers can tailor interventions and policies more precisely to combat cyberbullying. This study holds significance in addressing cyberbullying within online gaming communities. It provides practical guidance for students, game developers, and policymakers by identifying effective prevention methods and underscores the importance of cybersecurity integration.

INTRODUCTION

The evolution of the game industry has made it one of the most promising markets in the digital world. Additionally, there are more than two billion users of online games globally, making them a tremendously popular leisure activity. Experts anticipate the global count of online game players to reach 3.07 billion in 2023, driven by a 5.6% year-on-year growth rate. Asia is the largest gaming market, boasting 1.6 billion gamers, followed by Europe (Gilbert, 2023). Gaming is no longer confined to a specific age group and has become a ubiquitous part of modern culture enjoyed by people of all ages. (Yew, 2023) has described the trend of online gaming as increasing in Malaysia, with more than half of the Malaysian population being gamers who have either played or are still playing games.

Moreover, (Dodge, 2022) has reported that various games are available now, usually categorized based on their characteristics and objectives, such as sports, quizzes, simulators, role-playing games, adventures, and action games. The top online games in 2022 include Mobile Legend, PUBG: Battlegrounds, Minecraft, Apex Legends, Fortnite Battle Royale, Call of Duty, Crossfire, and Dungeon Fighter Online. Players can communicate through chat systems, voice, or in-game messaging, fostering teamwork and collaboration. They can access these games through various platforms, such as computers, consoles, smartphones, or tablets.

Next, (Li et al., 2023) emphasized that online games can reduce depression and stress, increase happiness, and enhance cognitive skills such as memory and mental agility. She also highlighted that online games, easily accessible and playable quickly, can improve players' moods, encourage relaxation, and help alleviate anxiety. However, (Umam et al., 2021) has explained excessive engagement in online games can lead to negative consequences such as addiction, social isolation, decreased physical activity, mental health, impaired academic performance, and potential exposure to inappropriate content or online predators.

Cyberbullying is an effect of addictive and frequent online gaming (Nur Utama et al., 2023). Cyberbullying in online games refers to oppressive behavior driven by emotional motives, impacting mental health and potentially leading to suicide, yet victims often feel powerless to act against it. In online games, cyberbullying involves three roles: perpetrators, bystanders, and victims games. Perpetrators are individuals who engage in cyberbullying behavior, intentionally causing harm or harassment to others. Bystanders are those who witness cyberbullying incidents but do not actively participate. Victims get bullied by perpetrators.

The Theory of Reasoned Action (TRA) is a cognitive theory developed by (Fishbein et al., 1980) to explain and predict human behavior. It encompasses belief, attitude, and subjective norm elements that can shape an individual's intention to engage in a particular behavior. Belief refers to an individual's perception or conviction on a specific behavior or outcome, attitude represents an individual's overall evaluation or assessment of behavior, which can be positive or negative, and subjective norm (SN) refers to an individual's perception of social pressure or influence from others regarding a specific behavior. The theory of Planned Behavior (TPB) is an extension of the TRA, and TPB was developed to improve TRA by incorporating the new perceived behavioral control (PBC) construct (Ajzen, Icek., 1991). He has explained that PBC stands for the person's belief that they can act, and it helps to describe situations in which behavior intentions alone are not entirely determinant of behavior due to restrictions on human control.

A range of studies have applied the TPB to understand cyberbullying. (Santre & Siriporn, 2021) found that the TPB's main variables—attitude, subjective norms, and perceived behavioral control—significantly influence cyberbullying intention. However, (Jafarkarimi et al., 2017) found that subjective norms and overall gain were the most significant determinants. Gender differences were also noted in the impact of these determinants. Previous studies have not examined cyberbullying that occurs among adolescents in online games, despite the prevalence of cyberbullying in these environments.

The Malaysia Cyber Security Strategy 2020-2024 outlines five key pillars and twelve strategies to fortify cybersecurity within the country (Majlis Keselamatan Negara, 2020). These pillars encompass effective governance and management, strengthening legislative frameworks and enforcement, catalyzing innovation and industry growth, enhancing capacity, awareness, and education, and fostering global collaboration. Strategies within these pillars range from improving national cybersecurity governance, updating and enforcing cyber laws, promoting research and development, nurturing a skilled cybersecurity workforce, raising public awareness, and engaging in international cooperation. However, a lack of research studies still explicitly explores the intersection of cyberbullying in online games, the integration of cybersecurity strategies, and the TPB. This study determines specified preventions in cyber security strategies to be adapted in TPB to combat cyberbullying in online games.

Practically, researchers have explored some aspects of cyberbullying (Cabrillos et al., 2023), but there is still a lack of detailed discussion on practices related to cybersecurity strategies. There are no specific guidelines on secure cyberbullying online games in line with cybersecurity strategies. The research lacks effective implementation of cybersecurity strategies in online games to address cyberbullying. There is inconsistency in prevention methods, and some platforms lack user-friendly reporting options or clear policies on cyberbullying. Better stakeholder coordination is needed to close this gap and ensure consistent and comprehensive cybersecurity measures. Therefore, this study aims to construct a cyberbullying behavior model in online games by integrating cybersecurity strategies.

LITERATURE REVIEW

This section will describe a literature review related to the current study.

Cyberbullying in online games

Research has consistently shown that cyberbullying is a significant issue in online gaming environments. Cyberbullying in online games refers to aggressive behaviors exceeding game objectives, often normalized in gaming culture due to anonymity, and not consistently recognized as cyberbullying by participants (McInroy et al., 2017). (McInroy et al., 2017) found that toxic behavior and aggression, including cyberbullying, are prevalent in these spaces. This can take various forms, such as verbal abuse, exclusion, spreading rumors, and sharing personal information without consent. Three prominent roles cause cyberbullying in online games: the perpetrator, who intentionally harasses others; the bystander, who watches but doesn't participate; and the victim, who suffers from the bullying. Perpetrators use the anonymity of the Internet to target and hurt others, while bystanders can either help or make things worse by their actions or inaction. Victims endure emotional pain and social isolation from the bullying, feeling powerless. Cyberbullying can cause victims severe psychological and emotional distress. Mobile Legends and PUBG can lead to cyberbullying among players, who may face harassment and negative interactions in these games (Al Mawalia & Khefti, 2020). Then, (Huang et al., 2019) found that senior high school students and boys were more likely to engage in cyberbullying behavior in online gaming, indicating potential age and gender differences in cyberbullying perpetration.

Factors and impacts of cyberbullying in online games

Research on cyberbullying in online gaming environments has revealed several key factors and impacts. The top factors that nurtured the cyberbullying Act are game rank, competition, and envy (Ballard et al., 2017). Factors of cyberbullying in online games, such as anonymity, the lack of real-life consequences, and the absence of fear of punishment, are perceived as the primary causes of cyberbullying in these environments. These factors are further exacerbated by the prevalence of aggressive behavior and the normalization of such behavior within the gaming culture (McInroy et al., 2017).

A lot of impacts from cyberbullying via online games (Prasetyaningtyas et al., 2021) found that cyberbullying did not directly affect player motivation and performance but rather influenced player satisfaction. This suggests that the effects of cyberbullying may be more subtle and long-term. Next, mental health, constant harassment, insults, threats, and humiliation can lead to anxiety, depression, low self-esteem, and suicidal thoughts or actions. Cyberbullying disrupts the social fabric of online gaming communities. It creates a hostile and toxic environment that discourages positive interactions and collaboration among players. Cyberbullying can have legal ramifications. Depending on the severity of the harassment, it may violate laws related to harassment, hate speech, or stalking.

Intervention and prevention of cyberbullying in online games

A range of interventions have been proposed to prevent and address cyberbullying in online games. (Garaigordobil et al., 2018) highlights the effectiveness of educational programs in severe games in promoting positive bystander behavior and reducing cyberbullying. These interventions focus on increasing awareness of the harm caused by cyberbullying, developing social and emotional skills, and improving self-efficacy and prosocial skills. (Calvo-Morata et al., 2020) further emphasized the potential of serious games as practical tools for raising awareness and teaching strategies to address cyberbullying. However, (Andrea et al., 2018) highlighted the increased risk of cyberbullying victimization among adolescents who play online games, suggesting the need for targeted interventions in this specific context. (Baltezarević et al., 2023) emphasizes the role of parents in monitoring their children's digital activities while (Ge et al., 2023) suggests using machine learning algorithms to detect and prevent abusive language.

Utilization of theory planned behavior for prevention of cyberbullying in online games

TPB has been applied to cyberbullying research, with studies identifying attitude, subjective norms, and perceived behavioral control as crucial determinants of cyberbullying intentions (Santre & Siriporn, 2021). This study is adapted from (Santre & Siriporn, 2021), which utilized the TPB to comprehend cyberbullying, emphasizing the significance of beliefs in developing interventions. The TPB model suggests that behavior is influenced by three main factors: attitudes towards the behavior, subjective norms (perceived social pressure to perform or not perform the behavior), and perceived behavioral control (perceived ease or difficulty of performing the behavior) (Santre & Siriporn, 2021).

Based on the research framework, an individual's attitude is formed by behavioral beliefs (BB), which link behavior to specific emotional, normative, or ethical consequences or characteristics (Ajzen, Icek., 1991). However, (Santre & Siriporn, 2021) focuses on teenagers being involved in cyberbullying (perpetrator), so this recent study investigates the role of perpetrator, victim, and bystander because all roles are involved in online games. The emotions experienced by cyberbullying incidents are negative for victims and positive for bullies, but this correspondence is reversed when considering moral disengagement mechanisms. The moral feelings state of the perpetrator toward the victim play a role in fueling cyberbullying behaviour. Cyberbullying in online games can lead to adverse reactions from others, including peer influence, and some respondents in the study mentioned that cyberbullying had no impact on their personal lives. Various studies have been conducted to develop models and tools for automatically detecting and removing cyberbullying comments in-game forums. Defending behaviors are associated with mental health issues such as social anxiety and depressive symptoms, particularly in victims and bystanders (Dang et al., 2020). Based on recent and previous studies, the researchers have identified factors such as moral feeling, emotional response, influence of peer group, fear of disapproval by peers, perceived low risk of detection, and willingness to defend as elements that impact attitude within behavioral beliefs.

Subjective Norm (SN) refers to an individual's perception of societal or peer approval regarding a behavior shaped by their normative beliefs, as posited by (Ajzen, Icek., 1991). In recent studies, researchers proposed Malaysian cybersecurity strategies based on normative belief. According to previous studies, friends would find it ok if cyberbullied someone (Santre & Siriporn, 2021). However, it is essential to note that the influence of injunctive norms on cyberbullying can vary depending on the properties of the referent groups (Gan et al., 2023) (injunctive norm of peers). Parents play an essential role in moderating the relationship between strain and anger in adolescent cyberbullying behaviour (Pratiwi et al., 2020) (tolerance by adults). Sometimes, peer pressure from others in online gaming can encourage individuals to engage in cyberbullying (Maharjan et al., 2022) (social pressure from peers), and the study by (Febrianti et al., 2023) found that pro-cyberbullying descriptive class norms were positively correlated with cyber aggression among adolescents (descriptive norms from peers).

Perceived behavioral control (PBC) refers to an individual's perception of how easy or challenging it is to engage in a specific behavior. It is rooted in control beliefs, as outlined by (Ajzen, Icek., 1991). Control beliefs pertain to an individual's perceptions regarding factors that could either facilitate or hinder the performance of a specific behavior. In the context of cyberbullying, factors such as the perceived anonymity provided by the Internet and mobile phones and the lower perceived risk of being caught might facilitate engaging in such behaviour. Moreover, the absence of direct face-to-face interaction may reduce individuals' inhibitions, making them more inclined to say or do hurtful things.

Elements of cybersecurity strategies to combat cyberbullying in online games

The Malaysia Cyber Security Strategy 2020-2024 is a comprehensive framework that outlines the elements and strategies to enhance cybersecurity in Malaysia (Majlis Keselamatan Negara, 2020). Instead of the pillars and strategies of cybersecurity, several pillars and strategies may help reduce cyberbullying in online games. The cybersecurity strategy for Malaysia includes twelve (12) strategies and five (5) strategic pillars that will guide all planning and implementation for cybersecurity up to the year 2024 (See Figure 3):-

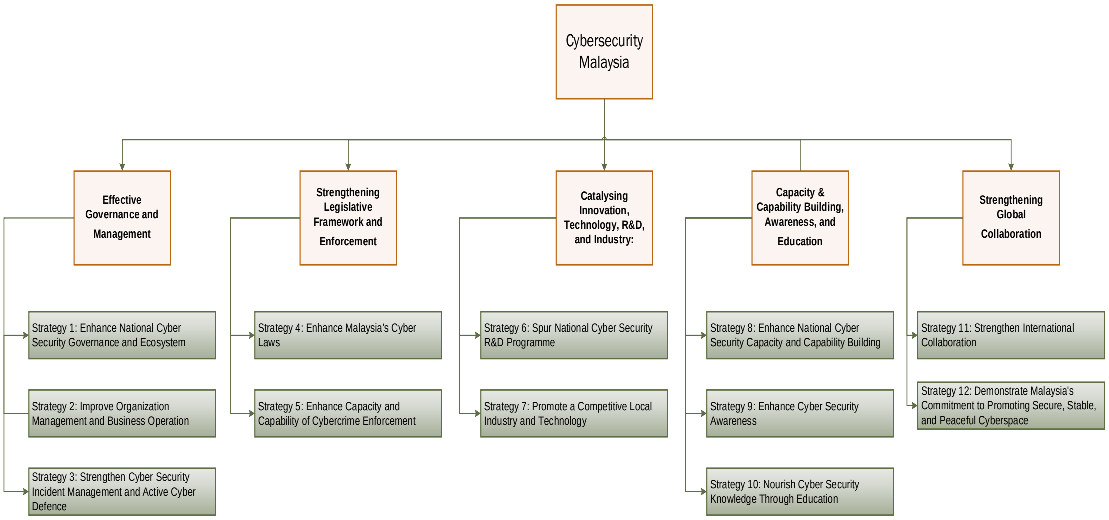
Cybersecurity Malaysia
Effective Governance and Management
Strengthening Legislative Framework and Enforcement
Catalysing Innovation, Technology, R&D, and Industry:
Capacity & Capability Building, Awareness, and Education
Strengthening Global Collaboration
Strategy 1: Enhance National Cyber Security Governance and Ecosystem
Strategy 2: Improve Organization Management and Business Operation
Strategy 3: Strengthen Cyber Security Incident Management and Active Cyber Defence
Strategy 4: Enhance Malaysia's Cyber Laws
Strategy 5: Enhance Capacity and Capability of Cybercrime Enforcement
Strategy 6: Spur National Cyber Security R&D Programme
Strategy 7: Promote a Competitive Local Industry and Technology
Strategy 8: Enhance National Cyber Security Capacity and Capability Building
Strategy 9: Enhance Cyber Security Awareness
Strategy 10: Nourish Cyber Security Knowledge Through Education
Strategy 11: Strengthen International Collaboration
Strategy 12: Demonstrate Malaysia's Commitment to Promoting Secure, Stable, and Peaceful Cyberspace

Figure 1: Cybersecurity strategies malaysia

The Malaysian Cyber Security Strategy has been formulated to strengthen national security and safeguard businesses (Majlis Keselamatan Negara, 2020). As the influence of the digital sector has grown significantly, these services have become a vital component of the nation's development. The cybersecurity services implemented through these strategies and plans play a crucial role in addressing cybercrimes and managing regulatory activities in the digital sphere (Majlis Keselamatan Negara, 2020).

As part of Pillar 2, which aims to fortify the legislative framework and enforcement mechanisms, Strategy 4 seeks to improve Malaysia's cyber laws to address current and future threats. This strategy involves a detailed review and enhancement of current legal frameworks to tackle cybercrime effectively, coupled with an assessment of the necessity for new laws in the realm of cybersecurity (Majlis Keselamatan Negara, 2020). Meanwhile, Strategy 5 aims to augment the capacity and capability of cybercrime enforcement agencies, ensuring they are well-equipped to manage cybercrimes, advanced threats, and organized crime syndicates (Majlis Keselamatan Negara, 2020).

In Pillar 4, dedicated to enhancing capacity and capability building and fostering awareness and education in cyber security, Strategy 8 aims to strengthen the national cyber security capacity and capability by devising a comprehensive plan for their development (Majlis Keselamatan Negara, 2020). This involves creating a detailed National Cyber Security Capacity and Capability Building Plan and formulating an integrated strategy for constructing adequate tools and technology. Strategy 9 seeks to refine the implementation approach of cyber security awareness programs to enhance cyber security awareness (Majlis Keselamatan Negara, 2020). This endeavor is to be facilitated by executing the National Cyber Security Awareness Master Plan. Furthermore, Strategy 10 endeavors to enrich cyber security knowledge through educational avenues by collaborating with the Ministry of Education to introduce cyber security as a subject in the primary, secondary, and tertiary level curricula (Majlis Keselamatan Negara, 2020).

Past studies have underscored the relation of Pillar 2 and 4 within the executed cybersecurity strategies in Malaysia for mitigating cyberbullying problems. Strengthening laws to address cyberbullying is complex, with varying approaches and challenges. (Kaluarachchi et al., 2020) highlights the need for legal reform, with (Kaluarachchi et al., 2020) advocating for a dedicated cyberbullying offense. Responsible use of technology, particularly among young people, parents, and schools, is also crucial in combating cyberbullying. The role of internet literacy in preventing cyberbullying has been emphasized, focusing on formal education. Collaborative approaches involving students, teachers, and parents effectively raise awareness and address cyberbullying. The need for a broad coalition of government, schools, police, and citizenry to combat cyberbullying has been highlighted (Ames et al., 2019).

METHODOLOGY

This section will describe the methodology implemented in this study.

Informants and procedures

The methodological approach encompassed several steps, beginning with one-on-one semi-structured interviews (n=4) and the identification of interviewees representing diverse perspectives relevant to the research topic, including a counselor, academician, cybersecurity expert, and game developer (see Table 1). The purposive sampling technique targeted those with professional expertise related to cyberbullying. Focusing on these individuals could carefully deconstruct and interpret their experiences, providing valuable insights for a deeper understanding of this intricate phenomenon, as suggested (Risardi & Alif Wildan, 2022). The interviews were approximately 60 minutes long, and the questions were related to cyberbullying behavior and cybersecurity strategies. Platforms like Google Meet and Webex were selected for interviews. Before interviews, informed consent was obtained from informants through prepared consent forms, ensuring adequate equipment availability for seamless communication. Interview sessions were recorded for documentation and subsequent analysis.

Table 1: Informant background

Informant	Background
A1	Developer Games
B1	Counselor
C1	Cybersecurity Expert
D1	Academician

Data analysis

Thematic analysis was employed to discern and interpret themes and patterns within the data set. The primary focus was on interview transcripts, serving as the fundamental units of analysis. Guided by the TPB and cybersecurity strategies, the thematic analysis aimed to identify specific elements within cybersecurity strategies that could be adapted to TPB in combating cyberbullying in online gaming environments. ATLAS.ti has been used to analyze data because it is a qualitative data analysis software capable of organizing various data types, including text, images, videos, and audio recordings. Visualization tools within ATLAS. ti, such as diagrams and word clouds, were leveraged to communicate research findings effectively. Furthermore, an interrater reliability evaluation involving three experts, comprising two academicians and a cybersecurity expert, bolstered the study's overall robustness.

FINDING AND DISCUSSION

The interviewees' findings show two themes in cybersecurity strategies for preventing online game cyberbullying. Most informants emphasize the importance of pillars 2 and 4: strengthening the legislative framework and enforcement. They also highlight the need to build capacity to combat cyberbullying in online games and raise awareness and education on cyberbullying.

Theme 1: Strengthening legislative framework and enforcement

Cyberbullying prevention in online games will succeed by enhancing current measures, and future regulatory efforts should focus on revising existing regulations. This action could minimize the impact of online games and provide sanctions for criminal behaviour (Ahmad et al., 2022). Findings from current research support this statement. The question is: Are there any acts or laws related to cyberbullying, especially concerning online platforms or games?" All experts believe existing laws in Malaysia do not adequately address the issue of cyberbullying, and the lack of specific legislation leaves victims vulnerable and without legal recourse. It is suggested that there is an urgent need for new laws and regulations to address cyberbullying in Malaysia specifically.

"In Malaysia, there are several laws related to cybercrime, but they encompass online gaming. The current weakness of the law is the lack of specific focus on cyberbullying in online games within the cyber laws in Malaysia" (A1).

Other respondents also explained the weakness of the laws in Malaysia regarding cyberbullying laws regardless of where it occurs. C1 strongly agrees with emphasizing the importance of Pillar 2, which is strengthening the legislative framework and enforcement and its strategies in combating cyberbullying, especially in online gaming.

"Among those pillars, I feel that the second pillar, which is strengthening legislative framework and enforcement, is essential" (C1).

The existing laws concerning cyberbullying in Malaysia are insufficient, as there is no specific law that regulates cyberbullying. Therefore, the researcher inquired, "How can we enhance or intervene in improving laws, especially the need for new legislation or amending existing laws?". Most experts explained several cybercrime laws that can be applied to cyberbullying cases, such as the Communications and Multimedia Act 1998, the Personal Data Protection Act 2010, and the Penal Code. Expert B explained in detail the Communications and Multimedia Act 1998 sections as inciting publishing or sending offensive messages, publishing or sending false messages, causing discomfort or disturbance, spreading false information or deceiving, threatening safety, and sending messages that invade privacy.

"Although no specific laws govern cyberbullying, the Communications and Multimedia Act 1998 clauses allow legal action against cyberbullying perpetrators. For example, if an individual harasses and incites someone to the point where they become distressed, we can sue and fight in court" (B1).

"It is essential to be aware that cyberbullying perpetrators can also be prosecuted under the Defamation Act 1927 if they involve defamation or slander and spreading falsehoods through platforms such as Facebook, WhatsApp groups, or online games" (B1).

"In the Communications and Multimedia Act 1998, there are provisions related to misuse, access to the Internet, and content in Sections 211 and 233. However, the requirement for intent to be stated in these sections can be challenging in court, proving cases such as cyberbullying. Confirming someone's intent to commit a crime is complex in the virtual realm. There is a suggestion that there is no need for the intent requirement in the Communications and Multimedia Act. This is due to the difference between the intent requirement in the Communications and Multimedia Act and the Penal Code. The aim is to harmonize these provisions to avoid conflicts" (D1).

D1 emphasizes raising fines as it will positively impact gamers. They will not easily engage in cyberbullying and maintain good behavior while playing games.

"We need to strengthen existing acts. We need to examine and review the provisions in these acts, including increasing the severity of penalties and fines, to ensure they remain relevant. The government should focus on refining and improving administrative aspects, not just enacting new laws" (D1).

It is essential to strengthen existing laws because they positively impact society as social changes among teenagers increase with online gaming. Online gaming activity is growing due to the various online games accessible to teenagers today (Yuliana, Yuliana, 2022).

The government has undertaken various efforts to enhance the capacity and capability of cybercrime enforcement. These efforts include adopting technical measures developed by private entities for crime prevention, while the public perception of law enforcement's role in cybercrime prevention remains weak. Additionally, legal politics plays a significant role in enforcing cybercrime laws, as it is closely related to the political will and interests of the government.

"The government has introduced professional courses and implemented training in digital forensics and security auditing. The government aims to train tens of thousands of cybersecurity professionals, but currently, the recorded number is only about 13,000. This involves training and providing better resources to law enforcement agencies to ensure they can deal with cyber threats more effectively" (C1).

A1 pointed out the significance of ethics and personal data security in preventing legal violations, as data breaches can lead to unauthorized access and compromise privacy and trust, a concern evident in online gaming where cyberbullies exploit such breaches to acquire player data for malicious intent.

Theme 2: Capacity & capability building, awareness, and education

Cyberbullying in online gaming poses significant challenges, necessitating the integration of cybersecurity strategies to address this issue effectively (Seok and B. DaCosta, 2018). Building capacity and capability, raising awareness, and providing education are crucial in combating cyberbullying within gaming communities.

"I think the fourth pillar, enhancing capacity and capability building, awareness, and education, can also be considered in addressing cyberbullying issues" (D1).

All experts consider that cyberbullying in online games can have severe mental health impacts, including cases of suicide. It is crucial to clearly understand the current online risks associated with video games, as they offer rich interactive experiences and raise safety concerns.

The researcher asked, "How can these strategies prevent cyberbullying in online games?". D1 explains that this strategy involves efforts to build capacity and initiatives in the field of cybersecurity, which includes developing necessary tools and technologies through an integrated approach. In online games, A1 strongly advocates for enhancing existing guidelines. It supports the implementation of new ones, particularly emphasizing the importance of incorporating cybersecurity elements into game development practices. They believe developing a model with cybersecurity considerations is a good approach and beneficial and adds value to improving game development standards in Malaysia.

"We can improve the existing guidelines, and I agree and support the need to issue these new guidelines" (A1).

"That's why if we want to develop a game, we should have a specific guideline that we can follow. Every developer who wants to develop [a game] must have a special guideline so that the content does not exceed violence" (A1).

"However, in Malaysia, no company or government agency is specifically responsible for checking the content of games developed by developers, as there is no specific presence in this regard. At the same time, game developers in Malaysia can create games without particular guidelines and have the freedom to operate without strict scrutiny" (1A).

A1 also suggests utilizing the SKMM's Guidelines for the Production and Provision of Interactive TV Video Game Services as a foundational framework for improvement, advocating for adding elements focusing on behavior and cyberbullying issues in video games to enhance effectiveness. He also proposes leveraging video game narratives to convey messages that discourage cyberbullying, mainly targeting children, by positively influencing their behavior through engaging storylines. C1 highlights the current emphasis on addressing perceptions of cyberbullying over cybersecurity aspects, advocating for agreement on guidelines before gaming, and stresses the importance of developing a code of ethics as a preventive measure against cyberbullying despite potential non-compliance.

C1 underscores the importance of enhancing focus on privacy and data protection in gaming, emphasizing the need for additional measures to safeguard players' data from misuse or unauthorized sharing. They suggest implementing age classifications similar to those used in movies, such as PG 13 to 18, to ensure appropriate content for different age groups. Furthermore, they advocate for establishing ethical guidelines, particularly for professional players, to prevent cyberbullying and promote cyber safety in gaming environments. D1 suggested collaborative efforts from players, game management, and the gaming community are needed to create an environment free from cyberbullying and support players' mental and emotional well-being. He emphasizes that game developers should prioritize safeguarding user privacy by minimizing personal data collection, addressing cyberbullying through effective reporting mechanisms, and considering cultural influences to avoid promoting negative behaviors in games.

"For me, there needs to be collaborative efforts from players, game management, and the gaming community as a whole to create an environment free from cyberbullying and to support the mental and emotional well-being of players" (D1)

It is essential to take action to improve the system and proactively reduce the likelihood of online connections turning into harassment in online games. By investing in capacity building, nations can enhance their cyber-security capabilities and mitigate gaps based on wealth, ultimately contributing to the prevention of cyberbullying in online games.

The level of cybersecurity awareness among teenagers regarding cyberbullying in online games is a critical issue. Research highlights the importance of educating teenagers and children about cybersecurity threats, such as cyberbullying, to shield them from scams, phishing, and online harassment (Rahman et al., 2020).

"I feel there's no awareness among these people regarding cybersecurity, which isn't meaningful to them. Whether they are children, teenagers, or adults, when playing games, they won't think about this issue. But they will acknowledge it after they have been affected" (A1).

"Students need to know online games before they start playing. They need to understand the rules and policies of the online game to protect themselves from cyberbullying. Before starting the game, it is essential to understand its mechanics and developers" (B2).

Some research has highlighted enhancing cybersecurity awareness among teenagers and preventing cyberbullying in online games, initiating early dialogue, educating about risks, encouraging parental involvement, and utilizing educational gaming experiences (Rahman et al., 2020). However, the findings reveal various government-run programs to raise awareness about cybersecurity on online platforms.

"The government has conducted numerous awareness programs, including the Program Siber Madani, cyberbullying education, the importance of user self through cybersecurity programs, the digital citizenship concept, cyber ethics, self-regulation, and the digital initiative" (C1).

D1 highlights the importance of netizens in preventing cyberbullying in the gaming community. He recommends using social media sites like TikTok to enhance cybersecurity awareness by making pertinent topics go viral on Instagram, Twitter, and TikTok. He also notes that netizens may raise awareness of cyberbullying and pressure perpetrators to reform despite the danger of disproportionate or brutal responses.

The researcher asked, "How suggestions for preventing cyberbullying and increasing cybersecurity knowledge through education?". D1 suggested one practical approach to enhancing awareness of cyberbullying and cybersecurity is integrating school education, where students are educated on legal compliance and equipped with an understanding of the influence and risks of cyberbullying, particularly within online gaming, emphasizing distinctions between virtual environments and real-life contexts. A lot of research consistently highlights the importance of education in combating cyberbullying, specifically the role of teachers in promoting awareness and understanding among students (Choi et al., 2021).

"It is essential to provide education and raise awareness among individuals about the influence and risks of cyberbullying associated with online gaming. They should be taught to understand the difference between gaming and the real world" (D1).

B1 explained that the efforts to address cyberbullying and enhance cybersecurity awareness in schools could be expanded by collaborating with experts, law enforcement, and cybersecurity organizations to provide workshops for students and staff and offer cybersecurity training for teachers, thereby augmenting existing counseling services and awareness campaigns.

"I feel that what can be done has already been implemented, including counselors providing counseling services and psychosocial support to students who are victims of cyberbullying or involved in cyberbullying activities. Furthermore, launching cyber safety awareness campaigns involving activities such as lectures, poster competitions, and creative educational activities" (B1).

"Perhaps my opinion needs to be expanded, such as collaborating with cybersecurity experts, law enforcement agencies, and cybersecurity organizations to provide lectures and workshops to students and school staff, as well as offering cybersecurity training for teachers and school staff so that they understand cyber threats and how to protect students and educate them in this aspect" (B1).

D1 suggests that it may be necessary to establish a cybersecurity education website aimed at creating and managing a cybersecurity education platform. This platform would provide educational resources, information, and guidance to students, teachers, and parents. A1 highlights the initial lack of cybersecurity awareness among individuals, which often only becomes apparent after experiencing firsthand incidents.

Cyberbullying behavior model for online games by integrating cybersecurity strategies

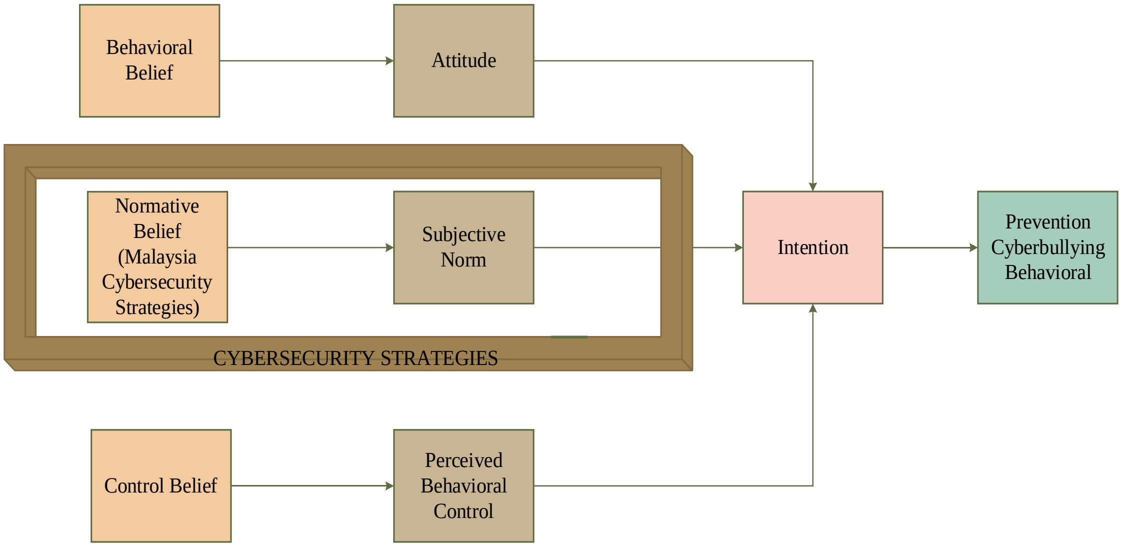
Behavioral Belief
Attitude
Normative Belief (Malaysia Cybersecurity Strategies)
Subjective Norm
CYBERSECURITY STRATEGIES
Intention
Prevention Cyberbullying Behavioral
Control Belief
Perceived Behavioral Control

Figure 2: Cyberbullying behavior model for online games by integrating cybersecurity strategies

The importance of integrating the pillars and strategies in TPB lies in their collective contribution to mitigating cyberbullying in online games. Strengthening legislative framework and enforcement enhances Malaysia's cyber laws, providing a legal basis for addressing cyberbullying incidents. Maintaining the capacity and capability of cybercrime enforcement ensures effective investigation and prosecution of cyberbullying cases. Capacity and capability building and awareness and education initiatives enhance national cybersecurity capacity and capability, creating a safer online environment. Additionally, efforts to improve cybersecurity awareness and nourish cybersecurity knowledge through education are crucial in empowering individuals to recognize, prevent, and report cyberbullying incidents effectively within online gaming communities.

CONCLUSION

In conclusion, this study examines the significant issue of cyberbullying in online gaming by integrating the TPB with cybersecurity strategies. Through an analysis of dimensions within TPB, crucial preventive factors influencing cyberbullying behavior in online gaming environments have been identified, including attitudes, subjective norms, and perceived behavioral control. In Malaysia's Cyber Security Strategy 2020-2024, specific elements have been investigated for integration into TPB, offering a multifaceted approach to combat cyberbullying effectively. A comprehensive cyberbullying behavior model tailored to online gaming has been proposed by synthesizing insights from TPB and cybersecurity strategies. With an emphasis on enhancing Malaysia's cyber laws and capacity for cybercrime enforcement, as well as enhancing capability building, awareness, and education, Malaysia can strengthen its cyber defenses and ensure a secure digital future for all, including the online gaming environment.

This study employs the TPB as its research framework and foundational reference, aiding researchers in addressing the primary question of identifying dimensions in TPB to prevent cyberbullying in online games. TPB is crucial in examining cyberbullying issues in online platforms, especially in online games, as it provides a comprehensive understanding of individual behavior and intention formation. This study advances theoretical knowledge regarding cyberbullying prevention strategies in online gaming by applying TPB. It enhances the applicability of TPB in addressing contemporary social issues. It underscores its relevance in guiding interventions to promote positive behaviors and mitigate cyberbullying incidents in online gaming environments. Additionally, this study extends the theoretical understanding of TPB by highlighting its effectiveness in addressing emerging challenges in digital spaces, enriching the academic discourse on cyberbullying prevention strategies.

The interview findings identified two main themes in strategies to prevent cyberbullying in online games. First, strengthening the legislative framework and enforcement is essential. Current laws in Malaysia are insufficient to address cyberbullying, especially in online gaming. Revising existing regulations and introducing new laws are recommended to provide specific protections and sanctions. Second, building capacity, raising awareness, and educating the public are crucial. This involves developing cybersecurity skills, increasing public awareness, and teaching young gamers about online risks. Additionally, implementing guidelines and ethical standards for game development and player behavior is necessary. Collaborative efforts among players, developers, and the government are recommended to enhance cybersecurity education and support systems, effectively combating cyberbullying.

This study is highly beneficial for people facing cyberbullying issues while gaming. Through this research, the researchers can identify the most effective strategies for preventing cyberbullying in games, particularly by integrating cybersecurity strategies. Additionally, it aids game developers in ensuring they create games suitable for students. Furthermore, the study contributes to the government's efforts to enhance cyberbullying awareness, especially in online gaming environments. By implementing the insights gained from this study, policymakers can develop more targeted interventions and policies to address cyberbullying effectively. This study is valuable for comprehensively addressing cyberbullying in online gaming communities. Furthermore, the study offers practical insights for students, game developers, and policymakers by identifying effective prevention strategies and highlighting the importance of cybersecurity integration. Through collaborative efforts informed by this research, stakeholders can work towards creating safer and more inclusive online gaming environments, ultimately fostering positive experiences for all users.

Limitations are inherent in any study, including this one, despite successfully addressing the research question and achieving the study objective. The first limitation revolves around the scope of the study, which focuses solely on the issue of cyberbullying prevention measures in online gaming. It would be beneficial for future research also to encompass factors and effects of cyberbullying in online gaming among students, as this issue continues to escalate annually. Secondly, the study's population is restricted to experts most involved in game cyberbullying prevention. However, future studies could expand to various age categories, from children to adults, given that almost all demographics engage in online gaming nowadays. Thirdly, the study primarily focuses on online games in general, and it would be advantageous for future research to narrow down to specific online games. Lastly, the study was conducted qualitatively with expert opinions on cyberbullying issues. Future research could aim to develop prototypes or systems that enhance awareness and prevention of online bullying.

Acknowledgment

This research was supported by the Ministry of Higher Education (MoHE) of the Fundamental Research Grant Scheme (FRGS) FRGS/1/2021/SS0/UUM/02/20 and Universiti Utara Malaysia (UUM).

REFERENCES

Ahmad, Wan Muhammad Iskandar Firdaus Wan, Siti Munirah Mohd, Amelia Natasya Abdul Wahab, Nurhidaya Mohamad Jan, Shafinah Kamarudin, and Hatika Kaco. "Permainan Dalam Talian: Trend Terkini di Kalangan Murid Sekolah Menengah di Malaysia." *International Journal of Education, Psychology and Counseling* (2022). https://doi.org/10.35631/IJEPC.745037

Ajzen, Icek. "The theory of planned behavior." *Organizational behavior and human decision processes* 50, no. 2 (1991): 179-211.

Al Mawalia, Khefti. "The impact of the Mobile Legend game in creating virtual reality." *Indonesian Journal of Social Sciences* 12, no. 2 (2020): 49-61. https://doi.org/10.20473/ijss.v12i2.22908

Ames, Heather, Claire Glenton, and Simon Lewin. "Purposive sampling in a qualitative evidence synthesis: A worked example from a synthesis on parental perceptions of vaccination communication." *BMC Medical Research Methodology* 19 (2019): 1-9. https://doi.org/10.1186/s12874-019-0665-4

Andrea, Christina, and Reny Yuliati. "Cyberbullying Victimization: The Risk of Playing Online Games on Adolescents." *Jurnal Komunikasi Global* 7, no. 2 (2018): 217-226. https://doi.org/10.24815/jkg.v7i2.12040

B. N. B. Yew, "To Play Or Not To Play : How Video Games Motivate Gamers In Malaysia To Play Benedict Ng Boon Yew Master Of Communication Faculty Of Creative Industries Universiti Tunku Abdul Rahman," Universiti Tunku Abdul Rahman, 2023.

Ballard, Mary Elizabeth, and Kelly Marie Welch. "Virtual warfare: Cyberbullying and cyber-victimization in MMOG play." *Games and Culture* 12, no. 5 (2017): 466-491. https://doi.org/10.1177/1555412015592473

Baltezarević, Vesna, Radoslav Baltezarević, and Ivana Baltezarević. "Cyber harassment of children with special reference to digital games." *Temida* 26, no. 2 (2023): 261-284. https://doi.org/10.36548/jitdw.2023.2.008

Cabrillos, Lenny E., Jegad D. Gapasin, Jeremy A. Marfil, and Vivencio L. Calixtro Jr. "Examining the effects of online games on the academic performance of BPEd students of Sultan Kudarat State University, Philippines." *Indonesian Journal of Educational Research and Technology* 3, no. 1 (2023): 13-18.

Calvo-Morata, Antonio, Cristina Alonso-Fernández, Manuel Freire, Iván Martínez-Ortiz, and Baltasar Fernández-Manjón. "Serious games to prevent and detect bullying and cyberbullying: A systematic serious games and literature review." *Computers & Education* 157 (2020): 103958. https://doi.org/10.1016/j.compedu.2020.103958

Choi, Eunsun, and Namje Park. "Can online education programs solve the cyberbullying problem? Educating south korean elementary students in the covid-19 era." *Sustainability* 13, no. 20 (2021): 11211. https://doi.org/10.3390/su132011211

Dang, Jianning, and Li Liu. "When peer norms work? Coherent groups facilitate normative influences on cyber aggression." *Aggressive behavior* 46, no. 6 (2020): 559-569. https://doi.org/10.1002/ab.21920

Dodge, D. "The Definitive Guide to Video Game Genres and Game Types." *URL: codakid. com/video-game-genres (дата звернення: 01.02. 2023)* (2022).

Febrianti, Rosa Wahyu, and Eppy Setiyowati. "Dampak Toxic Game Terhadap Cyber Bullying." *Jik Jurnal Ilmu Kesehatan* 7, no. 1 (2023): 70-76. https://doi.org/10.33757/jik.v7i1.652

Fishbein, Martin, and Icek Ajzen. "Predicting and understanding consumer behavior: Attitude-behavior correspondence." *Understanding Attitudes and Predicting Social Behavior* 1, no. 1 (1980): 148-172.

Gan, Xiong, Ke-Nan Qin, Guo-Xing Xiang, and Xin Jin. "The relationship between parental neglect and cyberbullying perpetration among Chinese adolescent: The sequential role of cyberbullying victimization and internet gaming disorder." *Frontiers in public health* 11 (2023): 1128123. https://doi.org/10.3389/fpubh.2023.1128123

Garaigordobil, Maite, and Vanesa Martínez-Valderrey. "Technological resources to prevent cyberbullying during adolescence: The cyberprogram 2.0 program and the cooperative cyber 2.0 videogame." *Frontiers in Psychology* 9 (2018): 353802. https://doi.org/10.3389/fpsyg.2018.00745

Huang, Chiao Ling, Shu Ching Yang, and Lu Sheng Hsieh. "The cyberbullying behavior of Taiwanese adolescents in an online gaming environment." *Children and Youth Services Review* 106 (2019): 104461. https://doi.org/10.1016/j.childyouth.2019.104461

Jafarkarimi, Hosien, Robab Saadatdoost, Alex Tze Hiang Sim, and Jee Mei Hee. "Cyberbullying among students: An application of Theory of Planned Behavior." In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, pp. 1-6. IEEE, 2017., https://doi.org/10.1109/ICRIIS.2017.8002521

Kaluarachchi, Chintha, Matthew Warren, and Frank Jiang. "Responsible use of technology to combat cyberbullying among young people." (2020).

Li, Feiyue, Di Zhang, Suowei Wu, Rui Zhou, Chaoqun Dong, and Jingjing Zhang. "Positive effects of online games on the growth of college students: A qualitative study from China." *Frontiers in Psychology* 14 (2023): 1008211. https://doi.org/10.3389/fpsyg.2023.1008211

Maharjan, Rocky, and Laxmi Gurung. "Cyberbullying and its Relationship with Smartphone Addiction." *Mangal Research Journal* (2022): 73-82. https://doi.org/10.3126/mrj.v3i1.51659

Majlis Keselamatan Negara, "Malaysia Cyber Security Strategy 2020-2024," 2020, [Online]. Available: https://asset.mkn.gov.my

McInroy, Lauren B., and Faye Mishna. "Cyberbullying on online gaming platforms for children and youth." *Child and Adolescent Social Work Journal* 34 (2017): 597-607. https://doi.org/10.1007/s10560-017-0498-0

N. Gilbert, "Number of Gamers Worldwide 2022/2023: Demographics, Statistics, and Predictions," *financesonline*, 2023. https://financesonline.com/number-of-gamers-worldwide/ (accessed February 26, 2023).

Nito, Joae Brett, Onieqie Ayu Dhea Manto Paul, and Dewi Wulandari. "Hubungan Riwayat Bullying (Korban) Tradisional Dengan Kejadian Cyberbullying Pada Mahasiswa." *NERS Jurnal Keperawatan* 18, no. 2 (2022): 58-67. https://doi.org/10.25077/njk.18.2.58-67.2022

Nur Utama, Herfian, Sidiq Setyawan, and M. I. Kom. "Perilaku Cyberbullying Dalam Game Online (Analisis Kualitatif Deskriptif Harassment Pada Game League Of Legends Wild Rift)." PhD diss., Universitas Muhammadiyah Surakarta, 2023.

Prasetyaningtyas, Sekar Wulan, and Aldo Prayogo. "The Effect of Cyberbullying in Multi-Player Online Gaming Environments: Gamer Perceptions." In *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS*, pp. 244-249. IEEE, 2021. https://doi.org/10.1109/ICIMCIS53775.2021.9699130

Pratiwi, Riska, and Yeni Karneli. "The contribution of online gaming and peer conformity to student bullying behavior." *Jurnal Aplikasi IPTEK Indonesia* 4, no. 3 (2020): 155-161. https://doi.org/10.24036/4.34375

Rahman, Nurul Amirah Abdul, Izzah Hanis Sairi, Nurul Akma M. Zizi, and Fariza Khalid. "The importance of cybersecurity education in school." *International Journal of Information and Education Technology* 10, no. 5 (2020): 378-382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Risardi, Alif Wildan. "Indonesian Legal Framework Related to Online Game Phenomena: A Criminological Review." *Rechtsidee* 11 (2022): 10-21070. https://doi.org/10.21070/jihr.v11i0.802

S. Ge, J. Wu, J. Xue, and C. Zhang, "Analysis of Bystander Intervention Behavior in Chinese Adolescents' Cyberbullying in Post-epidemic Era," Lect. Notes Educ. Psychol. Public Media, vol. 6, no. 1, 2023, https://doi.org/10.54254/2753-7048/6/20220351

S. Seok and B. DaCosta, "The Cyber Awareness of Online Video Game Players," Int. J. Cyber Res. Educ., vol. 1, no. 1, 2018, https://doi.org/10.4018/IJCRE.2019010108

Santre, Siriporn. "Theory of planned behavior in cyberbullying: A literature review." *International Journal of Research Reviews in Applied Sciences* 8, no. 11 (2021): 234-239. https://doi.org/10.52403/ijrr.20211131

Umam, Khotibul, and Abdul Muhid. "Sisi Negatif Game Online Perspektif Islam dan Psikologi Islam." *Psikoislamedia: Jurnal Psikologi* 5, no. 2 (2021): 153-167. https://doi.org/10.22373/psikoislamedia.v5i2.7071

Yuliana, Yuliana. "The importance of cybersecurity awareness for children." *Lampung Journal of International Law* 4, no. 1 (2022): 41-48. https://doi.org/10.25041/lajil.v3i2.2526