Intellectual Discourse

Volume 31 Number 1 2023

Editor-in-Chief
Danial Mohd Yusof (Malaysia)

Associate Editors
Anke Iman Bouzenita (Oman)
Khairil Izamin Ahmad (Malaysia)
Saodah Wok (Malaysia)

Editor
Tunku Mohar Mokhtar (Malaysia)

Book Review Editor
Mohd. Helmi Bin Mohd Sobri (Malaysia)

Editorial Board
Abdul Kabir Hussain Solihu (Nigeria)
Syed Farid Alatas (Singapore)
Badri Najib Zubir (Malaysia)
Thameem Ushama (Malaysia)
Daniel J. Christie (USA)
Habibul H. Khondker (UAE)
Hazizan Md. Noon (Malaysia)
Fahimul Quadir (Canada)
Hussain Muntalib (Singapore)
Habib Zafarullah (Australia)
Ibrahim M. Zein (Qatar)
John O. Voll (USA)
James D. Frankel (China)
Muhammad al-Ghazali (Pakistan)
Kenneth Christie (Canada)
Muhammad K. Khalifa (Qatar)
Nor Faridah Abdul Manaf (Malaysia)
Redzuan Othman (Malaysia)
Rahmah Bt Ahmad H. Osman (Malaysia)
Serdar Demirel (Turkey)

Intellectual Discourse is a highly respected, academic refereed journal of the International Islamic University Malaysia (IIUM). It is published twice a year by the IIUM Press, IIUM, and contains reflections, articles, research notes and review articles representing the disciplines, methods and viewpoints of the Muslim world.


ISSN 0128-4878 (Print); ISSN 2289-5639 (Online)

https://journals.iium.edu.my/intdiscourse/index.php/id
Email: intdiscourse@iium.edu.my; intdiscourse@yahoo.com

Published by:
IIUM Press, International Islamic University Malaysia
P.O. Box 10, 50728 Kuala Lumpur, Malaysia
Phone (+603) 6196-5014, Fax: (+603) 6196-6298
Website:http://iiumpress.iium.edu.my/bookshop
Contents

Note from the Editor 1

Research Articles

Validation of a Sejahtera Living Index Using the Rasch Model
Muhammad Faris Abdullah
Mohamad Sahari bin Nordin
Suhailah binti Hussien
Norhayati Mohd. Alwi
Noor Suzilawati binti Rabe 7

Investigating Ismāʿīl Rājī al-Fārūqī’s Methodology in the Study of Christianity through Selected Textual Analysis from His Christian Ethics
Fatmir Shehu 31

Paradoxical and Insufficient? Gender Quotas and Placement Mandates in Bosnia and Herzegovina’s 2020 Local Elections
Mirsad Karić
Šejma Aydin
Huseyin Korkut
Muhidin Mulalić 57

Gestalt and Semiotic Analyses of Brand Communication on Disability Inclusion: The Case of Malaysia and the US
Aida Mokhtar
Faiswal Kasirye 83

Understanding the Decline of Pakistan-US Alliance and the Growing Influence of China in Pakistan
Roy Anthony Rogers
Noraiz Arshad
Iftikhar Ali 113
Let’s Think They are Safe Online!
A Malaysian Perspective on The Classification of Children’s Cyber Risks
Sarina Yusuf  
Misha Teimouri  
Muhamad Shamsul Ibrahim  
Nan Zakiah Megat Ibrahim  
Syahida Mohd Nazri  
Stephanie Ann Victor

Social Media Use for English Learning in Southeast Asia:  
A Systematic Review  
Farah Fazlinda Mohamad  
Khazaila bt Zaini  
Nur Syahidatul Idany

Maqāṣid al-Sharī’ah as Goal Framing for Sustainable Behaviours: A Conceptual Framework  
Ali Mehellou  
Mohamad Saifudin Mohamad Saleh  
Bahiyah Omar

Faith in The Time of Coronavirus:  
A Corpus-assisted Discourse Analysis  
Siti Aeisha Joharry

COVID-19: Analysing the Principle and Application of Iʿtibār Maʿālāt in the Selected Fatwas Issued by the Malaysian National Council for Islamic Religious Affairs (MKI)  
Abdul Manan Ismail  
Ahmad Syukran Baharuddin  
Muhammad Hazim Ahmad

The Challenges of Civil Society Organisations:  
NGO-isation of Resistance in Malaysia?  
Sharifah Nursyahidah Syed Annuar  
Muhamad Takiyudin Ismail
The Authenticity of Theology in Scientific and Technological Thinking
Anhar Anshory
Ahmad Faizuddin Ramli
Ramli Awang

Research Notes
The Seminar on Da‘wah in Kuala Lumpur in 1977 and the Emergence of Hijab Awareness in Indonesia
Alwi Alatas
Agus Setiawan
Achmad Sunjayadi
Yunadi Ramlan

Book Review
### Transliteration Table: Consonants

<table>
<thead>
<tr>
<th>Arabic</th>
<th>Roman</th>
<th>Arabic</th>
<th>Roman</th>
</tr>
</thead>
<tbody>
<tr>
<td>ب</td>
<td>b</td>
<td>ط</td>
<td>t</td>
</tr>
<tr>
<td>ت</td>
<td>t</td>
<td>ظ</td>
<td>z</td>
</tr>
<tr>
<td>ث</td>
<td>th</td>
<td>ع</td>
<td>’</td>
</tr>
<tr>
<td>ج</td>
<td>j</td>
<td>غ</td>
<td>gh</td>
</tr>
<tr>
<td>ح</td>
<td>h</td>
<td>ف</td>
<td>f</td>
</tr>
<tr>
<td>خ</td>
<td>kh</td>
<td>ق</td>
<td>q</td>
</tr>
<tr>
<td>د</td>
<td>d</td>
<td>ك</td>
<td>k</td>
</tr>
<tr>
<td>ذ</td>
<td>dh</td>
<td>ل</td>
<td>l</td>
</tr>
<tr>
<td>ر</td>
<td>r</td>
<td>م</td>
<td>m</td>
</tr>
<tr>
<td>ز</td>
<td>z</td>
<td>ن</td>
<td>n</td>
</tr>
<tr>
<td>س</td>
<td>s</td>
<td>ه</td>
<td>h</td>
</tr>
<tr>
<td>ش</td>
<td>sh</td>
<td>و</td>
<td>w</td>
</tr>
<tr>
<td>ص</td>
<td>š</td>
<td>ء</td>
<td>’</td>
</tr>
<tr>
<td>ض</td>
<td>ḍ</td>
<td>ي</td>
<td>y</td>
</tr>
</tbody>
</table>

### Transliteration Table: Vowels and Diphthongs

<table>
<thead>
<tr>
<th>Arabic</th>
<th>Roman</th>
<th>Arabic</th>
<th>Roman</th>
</tr>
</thead>
<tbody>
<tr>
<td>ﺹ</td>
<td>a</td>
<td>ﺹ، ﻞ</td>
<td>an</td>
</tr>
<tr>
<td>ﺟ</td>
<td>u</td>
<td>ﻞ</td>
<td>un</td>
</tr>
<tr>
<td>ﻓ</td>
<td>i</td>
<td>ﻞ</td>
<td>in</td>
</tr>
<tr>
<td>ض، ض، ﺟ، ﺟ</td>
<td>ā</td>
<td>ﻞ</td>
<td>aw</td>
</tr>
<tr>
<td>ﻉ</td>
<td>ū</td>
<td>ﻞ</td>
<td>ay</td>
</tr>
<tr>
<td>ﻦ</td>
<td>ī</td>
<td>ﻞ</td>
<td>(in final position)</td>
</tr>
<tr>
<td>ﻦ</td>
<td>iyy</td>
<td>ﻞ</td>
<td>(in final position)</td>
</tr>
</tbody>
</table>

Source: ROTAS Transliteration Kit: http://rotas.iium.edu.my
Let’s Think They are Safe Online!  
A Malaysian Perspective on The Classification of Children’s Cyber Risks

Sarina Yusuf*  
Misha Teimouri**  
Muhamad Shamsul Ibrahim***  
Nan Zakiah Megat Ibrahim****  
Syahida Mohd Nazri*****  
Stephanie Ann Victor******

Abstract: Children currently spend more time on the Internet and corresponding technologies to socialise virtually and play video games. Scholars have not reached a consensus on whether children’s participation in such recreational activities is beneficial or detrimental. Although Malaysian parents are concerned about the digital threats that may be encountered by their children, most of the detriments remain unknown. Children still hesitate to inform their
families about their online exposure to inappropriate content, such as cybersex and pornography, which remain taboo subjects in Malaysian households. This study performed a descriptive analysis to determine the risk factors associated with children’s internet use with 420 school-going children aged from 9 to 16 years around Selangor. Resultantly, children were highly exposed to unwanted exposure to pornography (17.4 %), potentially dangerous user-generated content (9 %), sexting (8.8 %), personal data misuse (6.4 %), cyber grooming (3.3 %), and cyberbullying (1.7 %) in the past 12 months of using the Internet.

**Keywords**: cyberbullying, digital generation, personal data misuse, sexting, unwanted exposure to pornography

**Introduction**

The Internet has transformed adolescents from a physical world to a virtual reality. Youths are more attracted to the leisure activities derived from the Internet, such as socialising, playing games, and watching television. In this vein, children denote the highest number of internet users. A survey revealed that 75% of internet users worldwide were under 24 years old (Statista, 2023). Similarly, 73% of internet users in
Asia-Pacific were under 24 years of age (Statista, 2023). Over 90% of the people in Malaysia use the Internet daily, not unlike other countries (UNICEF, 2020). Specifically, more than 80% of these users are children under 15 years old (UNICEF, 2020). Children in Malaysia could easily access the Internet through personal computers, laptops, tablets, and smartphones, specifically following the emergence of COVID-19, which has characterised the Internet as a new norm in the education system. Students must connect to the Internet for educational activities. Despite the advantages of using the Internet (seamless information and knowledge attainment), children are susceptible to multiple internet-associated risks, such as cybercrime and cyberbullying.

Online risks generally denote a set of “intended or unintended” and “wanted or unwanted” experiences that adversely impact Internet users (Zlamal et al., 2020). Children who receive inappropriate content, participate in risky behaviour with communication, or contribute to harmful content or communication are vulnerable to online pornography or sexual solicitations (Keen et al., 2020; Kwan et al., 2020), online harassment and cyberbullying (Bakar et al., 2018; Blaya et al., 2020; Costello et al., 2020), exposure to hateful content (Costello et al., 2020), X-rated contents, such as “rough sex” on the Internet (Vogels & O’Sullivan, 2019), violent or coercive pornography (Landripet et al., 2019), and other desired or undesired and inappropriate behaviour arising from internet use.

Malaysian families are relatively aware of cyber dangers (Ahmad et al., 2019). As 80% of Malaysian children from 10 to 17 years old have access to inappropriate content, including pornography (Ahmad et al., 2019), Malaysian parents believe that their children may encounter such content. Nevertheless, most children are susceptible to online risks following their parents’ lack of supervision. Almost 89% of adolescents between 13 and 17 years old, who were victims of internet grooming, fell prey to inappropriate acts (New Strait Times, 2019). Based on a national survey, 83% of students in Malaysia were exposed to various types of online risks. Specifically, 70% of them were victims of online harassment, while 64% received or sent improper messages or images online (DiGi Cyber Safe report, 2014). It is deemed challenging for parents to keep constant surveillance of their children, who are required to use portable devices (smartphones) to perform educational activities.
The Malaysian government has taken initiatives to decrease cyber risks by drafting laws on cyberbullying, such as cybersecurity outreach (Digital, 2020). Much research on cyber risk and cyberbullying has also been conducted. For example, Kee et al. (2022) investigated cyberbullying predictors through social media, while Ooi et al. (2022) examined the factors associated with adolescent cyberbullying. Notwithstanding, cyberbullying, and cyber risk in Malaysia are steadily increasing despite extensive research in this area and governmental initiatives. A recent survey revealed that “Malaysia is 2nd in Asia for youth cyberbullying” (Star, 2022). Overall, the question of how to decrease cyberbullying and cyber risk in Malaysia remains unaddressed.

The significant rise in internet-using children has garnered much attention from scholars and regulatory bodies. As such, this study aims to investigate the classification of cyber risk and its subsequent effect on children’s life. The empirical outcomes would facilitate regulatory authorities to establish and implement relevant rules and regulations.

**Literature Review**

The increasing use of digital technologies has highlighted cyber risk as a growing concern for children (Bevan Jones, 2020). Children are vulnerable to cyberbullying following the anonymity and accessibility of digital technologies, which serve as a platform for harassment and abuse (Mkhize, 2021). Children who are victims of cyberbullying may experience depressive symptoms, anxiety, and low self-esteem (Zhong, 2021). Online predators, such as perpetrators who utilise social media and other digital platforms to groom and exploit children, are a significant cyber threat (Karadimce, 2023). Such manipulations could negatively affect the victim’s physical and mental health and future prospects.

A multidimensional approach involving parents, educators, and law enforcement proves necessary to safeguard children from cyber risk (Abd Rahman et al., 2022). Parents can play a pivotal role in supervising their children’s online activities and establishing guidelines for the safe and responsible use of digital technologies (Lamsal, 2022). Meanwhile, educators could equip students with digital literacy and cyber safety knowledge and skills to remain safe online (Nascimbeni & Vosloo, 2019). Law enforcement agencies that effectively identify and prosecute cybercriminals indicate that such conduct would not
be tolerated (Graham, 2023). Community members must collectively address cyber risk challenges and protect children from digital hazards (Jain et al., 2021). Overall, relevant statistics reveal a steady rise in cyber risks despite the efforts of academicians, law enforcement institutions, parents, and teachers to decrease such risks.

Cyber risk is generally considered an online security issue (HWEE, 2009). Nevertheless, several studies have classified this risk in terms of cyberbullying and cyber harassment (Quayyum et al., 2021). Despite much research on the cross-cultural variation in cyberbullying in different countries (Smith et al., 2018), most of the empirical works were performed in North America, Europe, and Australia (Hinduja & Patchin, 2013; Kowalski et al., 2014; Smith & Berkknun, 2017). These scholars conceded that the meaning and classification of cyber risk differed across nations, cultures, and norms. Existing cyber risk and cyberbullying studies in the Asian Pacific region also highlighted certain classification-related drawbacks. As numerous studies categorised cyber risk differently following their local culture, scope, and context (Kamaruddin et al., 2023; Smith et al., 2019), this study posited that cyber risk is different in Malaysia compared to other countries. Hua et al. (2019), who explored the linguistic features of cyberbullying in Malaysia, analysed the language used in cyberbullying incidents on social media platforms to identify patterns and characteristics that could distinguish cyberbullying from other online communication types. The authors evaluated a sample of cyberbullying messages gathered from social media platforms, with emphasis on linguistic features: syntax, lexical choices, and use of emoticons. Resultantly, cyberbullying messages frequently employed negative language and derogatory terms and emoticons to convey negative emotions. The authors suggested using these linguistic features to develop algorithms that could automatically identify and classify cyberbullying messages. Internalising the linguistic features of cyberbullying could develop effective strategies to prevent and address this issue locally and globally. Based on the study, most of the abusive remarks began with the word “Kepala”, which means head in Malay. Other local studies on cyberbullying (Adebayo et al., 2020; Sivabalan et al., 2020) were also conducted in Malaysia.

The definition of cyberbullying varies following the research context and purpose. In Malaysia, de-hijabbing (a voluntary act of removing the hijab) (Noor & HAMID, 2021) and its promotion is considered
cyberbullying (Noor & HAMID, 2021). Thus, cyberbullying could be characterised in terms of harassment, flaming, denigration, impression, exclusion, cyberstalking, and impersonation (Willard, 2007). Relevant scholars have investigated cyberbullying with different linguistic methods. For example, several researchers used natural language processing (NLP) and machine learning programme to detect the matching text. The bag-of-words approach, part-of-speech tagging, and grammar features were initially applied for detection purposes (Dinakar et al., 2011), followed by content-based features: lexical, syntactic, and sentiment information (Ptaszynski et al., 2016; Zhao et al., 2016).

Contrarily, some studies contended with the insufficiency of these methods and tools to detect cyberbullying given the pliability of the term, which changes based on the context (Zhong et al., 2022). Despite inconsistent statements about cyberbullying, the existing literature gap may be bridged by categorising cyberbullying based on profession, age, religion, and other demographic attributes. This research only included cybercrime categories and considered cyberbullying as inappropriate messages, receiving, or sending nasty messages, or being left out. Additionally, the study proposed cyberbullying as a personal insult and sexual harassment, albeit with insufficient literature to identify the cyber risk classification.

Classification of Cyber Risk

In line with the knowledge gaps, this study categorised the cyber risk type based on relevant literature and surveys:

(1) Cyberbullying includes inappropriate messages, receiving nasty messages, and being left out. The Child Online Safety Index (COSI) is a global think-tank institute that collected data from 145,426 children and adolescents in 30 countries between 2017 and 2019 as part of the DG Every Child project. Reportedly, 60% of children from 8 to 12 years old were generally exposed to cyber risks, with 45% of them experiencing cyber-bullying, 39% experiencing reputational risks, 29% exposed to risky (violent or sexual) content, 28% exposed to cyber threats, 17% experiencing risky contact (offline with strangers or sexual contact), 13% at risk for a gaming disorder, and 7% at risk for social media disorder (DGInstitute, 2020). The DG Lab Report (2020) disclosed Spain and Australia to have the highest rate
of Child Internet Safety Act, followed by Malaysia ranking second, Singapore ranking third, and Singapore ranking fourth.

(2) Sexting includes all received or sent inappropriate material, including images videos and text. Youth and Media (YaM) covers research and development initiatives among youths from 12 to 18 years old and digital technology whilst closely interacting with other teams at the Berkman Klein Cent. The dynamic global, social, and cultural environments impact the current discourse with input on new youth and digital media topics, whereby methodologies were introduced that could capture young adults’ experiences to contribute to the economic and social effects of novel technologies (YaM, 2020). The Berkman Center has initiated the Internet Safety Technical Task Force (ISTTF) project to identify sexual solicitation, online harassment, and problematic content as a subgroup of online risks and digital technology (Berkman Center for Internet & Society, 2008).

(3) Risky online conversation includes sending phone numbers and addresses or seeking someone for an intimate relationship. The Family Online Safety Institute (FOSI) surveyed adolescents from ages 13 to 17 and introduced classifications of teen identity theft, fraud, being tracked for marketing, being bullied, ugly or unflattering pictures posted, and security issues on the Internet (Family Online Safety Institute, 2013). The FOSI aims to promote a culture of responsibility online and encourages a sense of digital citizenship through research, resources, events, and special projects.

(4) Unwanted exposure to pornography includes all the unwanted materials in pornography, such as unwanted e-mails, unwanted obscene materials on messages or links, and similar encounters. The Youth Internet Safety Survey (YISS) group conducts another systematic study, which is repeated every five years in the United States. The YISS-1, YISS-2, and YISS-3 and the Fourth National Survey of Internet & Technology Facilitated Child Exploitation (Mitchell, 2020) were conducted in 2000, 2005, and 2010 to quantify younger Internet users’ unwanted
or problematic experiences, including unwanted exposure to pornography and sexual solicitation or harassment.

(5) Potentially harmful user-generated content includes all the content on danger or threat, such as bloody photos, videos related to being beaten up, and other related material, including images and texts. The Online Safety and Technology Working Group (OSTWG, 2010) defined the online risk categories as predator danger, cyberbullying, sexting, and inappropriate content.

(6) Personal data misuse includes data misuse activities, such as password misuse and being hacked. The European Kids Online survey, known as “EU Kids Online”, is a research network that interviewed European children and their parents from 25 European countries from 2006 to 2009. The EU kids online has since conducted periodic research among European children. The latest project reports were published (Smahel et al., 2020; Zlamal et al., 2020) to evaluate online opportunities and risks for children. Another study entitled ‘Be safe, Go online’ was conducted in a Malaysian university-grant project (2012-2015) to study Internet usage and online risks among 1800 respondents, including 800 Malaysian adolescents from 8 to 16 years and their parents (Daud et al., 2014; Teimouri et al., 2014; Yusuf et al., 2014). The study included the risk of hacking activities and data misuse.

Multiple studies have been conducted on cyber risk. To date, cyber risks imply security risks, such as information misuse or hacking. Regardless, other empirically-excluded categories indicate a knowledge gap in cyber risk categories. The current study proposed some additional categories to fill the literature gap. As this research was conducted in Malaysia, multiple factors (parenting style in Malaysia, educational situations, norms, culture and language) were regarded while proposing new cyber risk categories.

Research Methodology

This study adapted global classifications of online risks and measurements, a modified national-classification version of online risks to children in the Malaysian index, based on the ‘Be Safe, Go Online’
The risks were classified into (1) unwanted exposure to pornography (adapted from Wolak et al., 2007), (2) potentially harmful user-generated content, (3) sexting, (4) personal data misuse (adapted from Livingstone et al., 2012), (5) risky online conversation that asked children whether they had sought someone online to talk about sex, have sex, or sent a sexual photo or video (adapted from Baumgartner et al., 2010; Finkelhor et al., 2011), and (6) cyberbullying. This study provided a descriptive outcome of the risks (adapted from Livingstone et al., 2012).

The current work included 420 children from primary and secondary schools, with an average age of 12, in two districts of Selangor (Gombak and Sepang), Malaysia. Purposive sampling was used to select the respondents. Muslim students who spent most of their time with parents after school were selected for data collection. The respondents should have at least one social media ID used in the last 12 months. Lastly, only students who felt comfortable providing data were selected as respondents. As this study aimed to test the cyber risk classification, the intensity of intent usage was not considered. Counsellors suggested the children at their respective schools. Empirical data were gathered with a classroom-administered survey method. Each session lasted for approximately one hour, during which students were accompanied by two researchers who assisted and guided them.

The researchers were required to substitute explicit terms in their study questions pre-data collection in adherence to Malaysian cultural appropriation. In Malaysian culture (specifically in Muslim families), some cyberbullying terms were deemed inappropriate while conversing with someone. The respondents may feel shy to use them directly. Hence, these words were rephrased without altering the original meaning. The sexually-explicit language was replaced for questionnaire validation. For example, the phrase “having sex” was replaced with “having an inappropriate intimate relationship, while “showing sexual actions and content” and “naked photos” were substituted with “obscene pictures” and “obscene acts or materials,” respectively. The data collected was classified into three levels ranging from 1 (low) to 3 (high).

The demographic results revealed that most students (66 %) were females and Malay Muslims from 9 to 16 years old (74 %). Statistically, children frequently used the Internet after school (80%) or under
parental supervision (79 %). Male students were more susceptible to cyber threats compared to their female counterparts.

Findings

This study performed a descriptive analysis to confirm the cyber risk classification. Resultantly, over 36% of the students encountered something on the Internet that “made them feel uncomfortable, upset, or that they shouldn’t have seen it”, while almost 58 % of them indicated having not experienced unfavourable scenarios. Meanwhile, 6 % did not respond to the question. Additionally, 61 % agreed on being exposed to unsuitable content, while 32 % disagreed and 7 % did not respond to the questions.

Most of the respondents (82.6%) reported a low level of exposure to “unwanted exposure to pornography,” while 17.4% of them denoted a high level of exposure. Meanwhile, 91% encountered low exposure to “potentially hazardous user-generated material”, whereas 9% accounted for excessive exposure. Many adolescents (91.2%) demonstrated low exposure to “sexting,” while 8.8% reflected significant exposure. Personal data abuse accounted for 93.6% and 6.4% of low-exposure and high-exposure cases, respectively. Most of the young adults (96.7%) engaged in low-level sexual online activity, while a mere 3.3% engaged in high-level sexual online behaviour. A majority of the adolescents (98.3%) experienced modest levels of “cyberbullying”, while only 1.7% experienced severe levels of “cyberbullying”.

Table 1: Descriptive report of child cyber risks exposure

<table>
<thead>
<tr>
<th>Constructs/indicators</th>
<th>% of frequency</th>
<th>M</th>
<th>S.D</th>
<th>% of high-low rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unwanted exposure to pornography</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Unwanted obscene materials on the web</td>
<td>45 47 8</td>
<td>1.62</td>
<td>0.62</td>
<td></td>
</tr>
<tr>
<td>2. Unwanted e-mail or IM</td>
<td>69 26 5</td>
<td>1.35</td>
<td>0.57</td>
<td></td>
</tr>
<tr>
<td>3. Unwanted obscene materials on messages or links</td>
<td>67 31 2</td>
<td>1.35</td>
<td>0.52</td>
<td></td>
</tr>
<tr>
<td>4. Naked picture/inappropriate intimate relationship on message/link</td>
<td>80 19 1</td>
<td>1.20</td>
<td>0.43</td>
<td></td>
</tr>
<tr>
<td>5. Anyone asks to talk about inappropriate acts</td>
<td>82 17 1</td>
<td>1.18</td>
<td>0.40</td>
<td></td>
</tr>
<tr>
<td>6. Anyone asks to do inappropriate acts</td>
<td>91 9 0</td>
<td>1.09</td>
<td>0.30</td>
<td></td>
</tr>
<tr>
<td>Overall mean</td>
<td></td>
<td>1.30</td>
<td>0.47</td>
<td></td>
</tr>
<tr>
<td>Potentially harmful user-generated content</td>
<td></td>
<td></td>
<td>91.0</td>
<td>9</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>1 Seen bloody movies or photos</td>
<td>40</td>
<td>54</td>
<td>6</td>
<td>1.66</td>
</tr>
<tr>
<td>2 Seen people beaten up</td>
<td>64</td>
<td>31</td>
<td>5</td>
<td>1.65</td>
</tr>
<tr>
<td>3 Seen hate messages</td>
<td>80</td>
<td>18</td>
<td>2</td>
<td>1.40</td>
</tr>
<tr>
<td>4 Seen anorexia or bulimic</td>
<td>94</td>
<td>6</td>
<td>0</td>
<td>1.22</td>
</tr>
<tr>
<td>5 Talk about drugs</td>
<td>95</td>
<td>5</td>
<td>0</td>
<td>1.06</td>
</tr>
<tr>
<td>6 Ways of physical harming</td>
<td>95</td>
<td>5</td>
<td>0</td>
<td>1.05</td>
</tr>
<tr>
<td>7 Ways of committing suicide</td>
<td>97</td>
<td>3</td>
<td>0</td>
<td>1.03</td>
</tr>
<tr>
<td>Overall mean</td>
<td>1.30</td>
<td>0.41</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sexting</th>
<th></th>
<th></th>
<th>91.2</th>
<th>8.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Received inappropriate messages</td>
<td>80</td>
<td>20</td>
<td>0</td>
<td>1.20</td>
</tr>
<tr>
<td>(words, pictures, and videos)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Being posted inappropriate materials</td>
<td>80</td>
<td>20</td>
<td>0</td>
<td>1.20</td>
</tr>
<tr>
<td>3 Being sent inappropriate messages</td>
<td>85</td>
<td>15</td>
<td>0</td>
<td>1.15</td>
</tr>
<tr>
<td>4 Seen obscene images or videos</td>
<td>86</td>
<td>14</td>
<td>0</td>
<td>1.14</td>
</tr>
<tr>
<td>5 Seen other people perform obscene acts</td>
<td>86</td>
<td>14</td>
<td>0</td>
<td>1.14</td>
</tr>
<tr>
<td>6 Seen intimate images or videos in a</td>
<td>87</td>
<td>13</td>
<td>0</td>
<td>1.13</td>
</tr>
<tr>
<td>violent way</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Seen someone’s obscene images or videos</td>
<td>89</td>
<td>11</td>
<td>0</td>
<td>1.11</td>
</tr>
<tr>
<td>8 Seen obscene images or videos about</td>
<td>90</td>
<td>10</td>
<td>0</td>
<td>1.10</td>
</tr>
<tr>
<td>private parts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall mean</td>
<td>1.15</td>
<td>0.36</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal data misuse</th>
<th></th>
<th></th>
<th>93.6</th>
<th>6.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Misuse of password</td>
<td>81</td>
<td>18</td>
<td>1</td>
<td>1.30</td>
</tr>
<tr>
<td>2 Misuse of personal information you didn’t like</td>
<td>90</td>
<td>10</td>
<td>0</td>
<td>1.08</td>
</tr>
<tr>
<td>3 Being hacked</td>
<td>92</td>
<td>8</td>
<td>0</td>
<td>1.05</td>
</tr>
<tr>
<td>4 Misuse of personal information</td>
<td>95</td>
<td>5</td>
<td>0</td>
<td>1.05</td>
</tr>
<tr>
<td>5 Lost money by being cheated online</td>
<td>97</td>
<td>3</td>
<td>0</td>
<td>1.03</td>
</tr>
<tr>
<td>Overall mean</td>
<td>1.10</td>
<td>0.30</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risky online conversation</th>
<th></th>
<th></th>
<th>96.7</th>
<th>3.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Sent address or phone number to someone you only knew online</td>
<td>75</td>
<td>19</td>
<td>5</td>
<td>1.30</td>
</tr>
<tr>
<td>2 Search for someone to talk about intimate relationship</td>
<td>92</td>
<td>7</td>
<td>0</td>
<td>1.08</td>
</tr>
<tr>
<td>3 Search for someone to do intimate relationship</td>
<td>96</td>
<td>4</td>
<td>0</td>
<td>1.05</td>
</tr>
<tr>
<td>4 Sent obscene photos to someone you only knew online</td>
<td>98</td>
<td>2</td>
<td>0</td>
<td>1.02</td>
</tr>
<tr>
<td>Overall mean</td>
<td>1.10</td>
<td>0.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyberbullying</td>
<td>Yes</td>
<td>No</td>
<td>Score</td>
<td>Total</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-----</td>
<td>----</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>1 Received inappropriate messages that bothered you</td>
<td>80</td>
<td>19</td>
<td>1.20</td>
<td>1.7</td>
</tr>
<tr>
<td>2 Received nasty or hurtful messages</td>
<td>84</td>
<td>16</td>
<td>1.17</td>
<td>0.38</td>
</tr>
<tr>
<td>3 Received another nasty message that hurt you</td>
<td>89</td>
<td>11</td>
<td>1.12</td>
<td>0.33</td>
</tr>
<tr>
<td>4 Being left out or excluded</td>
<td>90</td>
<td>10</td>
<td>1.10</td>
<td>0.32</td>
</tr>
<tr>
<td>5 Received nasty or hurtful messages about yourself</td>
<td>92</td>
<td>8</td>
<td>1.08</td>
<td>0.29</td>
</tr>
<tr>
<td>6 Being threatened online</td>
<td>94</td>
<td>6</td>
<td>1.06</td>
<td>0.25</td>
</tr>
<tr>
<td>7 Being asked to talk about nasty acts</td>
<td>95</td>
<td>5</td>
<td>1.05</td>
<td>0.21</td>
</tr>
<tr>
<td>8 Being asked to show your private part</td>
<td>96</td>
<td>4</td>
<td>1.04</td>
<td>0.21</td>
</tr>
<tr>
<td>9 Received inappropriate messages encourage you to run away</td>
<td>97</td>
<td>3</td>
<td>1.03</td>
<td>0.16</td>
</tr>
<tr>
<td><strong>Overall score</strong></td>
<td></td>
<td></td>
<td>1.09</td>
<td>0.28</td>
</tr>
</tbody>
</table>

**Figure 1:** Malaysian classification of online risks model

**Discussion**

This study pioneers the purposing of cyber risk categories, all of which were confirmed based on the research outcome. Most of the
respondents reported encountering unwanted exposure to pornography, followed by sexting, and personal data misuse. Regardless, very few of them experienced risky online conversations and cyberbullying. As such, the study outcome confirmed six cyber risk categories as follows: unwanted exposure to pornography, potentially harmful user-generated content, sexting, personal data misuse, risky online conversation, and cyberbullying.

Unwanted exposure to pornography

This study considered unwanted exposure to pornography as unwanted material sent or received over the Internet. Empirically, 17.4% of the respondents encountered unwanted exposure to pornography following existing works on unwanted exposure to pornography (Henry, 2023; Kumar et al., 2016), which documented a high number of respondents encountering unwanted exposure to pornography. Despite a paucity of local studies on unwanted exposure to pornography, these empirical works underscored unwanted exposure as a primary issue (Teimouri et al., 2014). This problem may result from ineffective internet regulation and monitoring measures. Although the Malaysian government has enforced laws to regulate online content, these regulations are frequently disregarded. Many websites and online platforms continue operating without proper supervision. Unwanted exposure to pornography could significantly impact young people and increase their vulnerability to the adverse effects of exposure to explicit materials. Following past literature, exposure to pornography could instigate various problems, including addiction, desensitisation to sexual content, and distorted views of sexuality and relationships.

Potentially harmful user-generated content

In line with the study outcomes, only 9% of the respondents encountered potentially harmful user-generated content. Notwithstanding, past Malaysian studies revealed that most of the respondents encountered such content (Sofee et al., 2022). This contradiction may result from variances in the research definition and context. Following Sofee et al. (2022), user-generated content on social media encompassed harmful and fear-inducing elements. Nonetheless, the study did not incorporate other cyber risk materials, such as sexting and pornography. Hence, the results depended on the study definition and context. It is deemed necessary to increase public awareness of and education on responsible
online behaviour and the implications of online content by educating content creators and consumers on the significance of validating information pre-sharing, avoiding hate speech, and respecting people’s privacy and dignity.

**Sexting**

Resultantly, only 8.8% of the children encountered sexting issues. This finding contradicted past studies, which highlighted sexting as a primary construct of cyber risk (Goh et al., 2022). This inconsistency could be attributed to the study respondents (children), who might have been hesitant to discuss such topics. Sexting could instigate content-sharing without consent, which could induce humiliation, embarrassment, and cyberbullying or harassment in some cases. Such content could lead to further harm or exploitation when manipulated by strangers or criminals. Sexting could also be used as a form of coercion or grooming. For example, an individual may be pressured into sending explicit photos or videos to someone in a position of authority (teacher or employer), who could then use the materials for exploitation purposes.

**Personal data misuse**

Only 6.4% of students encountered issues with personal data misuse. The current study results varied from past literature, where many people experienced data misuse (Sudarwanto & Kharisma, 2022). This contradiction could result from differences in terms of definition and context. In Malaysia, data misuse incidents in the context of cyber risk for children proved to be lower.

**Cyberbullying and Risky Online Communication**

Relevant literature considers risky online communication as cyberbullying (Yusop & Al-Shami, 2021). Notwithstanding, this study regarded the concept from different categories. The results revealed a minimal number of students who encountered cyberbullying. Regardless, past literature posited cyberbullying as one of the key concerns in Malaysia (ASANAN et al., 2016). The current study outcomes may be different, as cyberbullying was considered separately with lesser factors. Nevertheless, relevant literature regarded more factors under cyberbullying. Overall, this study proposed cyberbullying as a cyber risk category to attract researchers’ and government bodies’ attention towards this issue.
Conclusion

The Internet has become part of children’s daily life following rapid advancements in digital technology, which may present new digital risks or threats. The current work expanded the current body of knowledge by proposing six cyber risk categories. Regardless, the risk associated with these categories is yet to be categorised. Researchers placed much emphasis on sex-related risks, sharing personal information with strangers, and cyberbullying as a range of online risks encountered by internet-using children. It is deemed crucial to categorise these activities for the government and regulatory bodies to undertake preventive measures and implement optimal strategies. For example, research by the Ministry of Science, Technology and Innovation, MCMC, and the Women, Family and Community Development Ministry, and Digi Telecommunication Sdn. Bhd provide useful insights into cyber risk among the target groups (Ahmad et al., 2019). The survey results revealed the need to extensively examine cyber risk and its associated categories for a sound understanding of the issue.

The Internet exposes children to both risks and opportunities. Based on the study finding, online risk exposure towards children between 9 and 16 years old in Malaysia was not very high as they “never or seldom experienced risks online”. Although the situation is not alarming, parents and society should seriously consider the online risks of “unwanted exposure to pornography” and “potentially harmful user-generated content” towards children. Over 50% of the current study respondents had been exposed to unwanted obscene materials (sexual content) on websites, while almost 60% had seen gory movies or photos and people being beaten up online. In addressing the concerns of family members, practitioners, and policymakers about the negative consequences of the online risks faced by children, it is deemed crucial to classify these risks: not all children feel uncomfortable, upset, or troubled upon encountering them (Zlamal et al., 2020). Strategies to mitigate such risks remain unexplored despite the digital threats encountered by internet-using children.

Due to sensitivity issues, the Malaysian Ministry of Education required the removal of some inappropriate or explicit words from the study questionnaire pre-data collection. For example, the phrase “having sex” was replaced with “having an inappropriate intimate relationship,”
while “naked pictures” and “showing sexual acts and content” were substituted with “obscene pictures” and “obscene acts or materials,” respectively. Hypothetically, the children may not have derived the actual meaning of the classified risks owing to the word replacements. Malaysian parents should be more realistic and open-minded as children-parent discussions on sexual matters remain taboo. Parents should face reality and initiate conversations with their children to create an awareness of online hazards and potential consequences. During data collection, the researchers observed the children’s reluctance to share their exposure to sexual content with parents and teachers. Visiting children at school in an isolated environment could also have influenced their responses. Future works could utilise different data collection methods to minimise the online risks encountered by children.

**Limitations and Recommendations**

The current work proposed six cyber risk categories that could be empirically examined. For example, potential researchers could investigate the intensity of these categories across multiple age groups. As this study did not investigate the risks associated with these categories, further research may analyse these risks in relation to various activities and their prevention. The present research only presented six cyber risk categories. As such, future works could introduce new classifications based on the Malaysian context and might use these classifications in a research framework. Given the current study limitations, which conducted a purposive study by confirming the cyber risk categories, further research may be performed to investigate these categories in different contexts and incorporate them into the research model. This empirical work proposed six broad categories of cyber risk. Hence, potential scholars could be more specific in considering these categories. As cyberbullying varies following the research context, each category should be sub-categorised based on future study contexts and aims. Prospective studies could perform sub-categorisation based on a country’s norms and culture, which was not included in this research.

**Acknowledgement**

Authors of this article would like to extend their utmost appreciation and gratitude to the Research Management and Innovation Centre of University Pendidikan Sultan Idris and the Ministry of Higher Education for funding the research project under the Fundamental Research Grant
Scheme (FRGS), code: FRGS/1/2021/SSO/UPSI/02/3 (2021-0137-106-02) that has led to the production of this article. The authors also wish to appreciate the continuance of support and unending guidance given that has led toward the success of the publication of this article.

References


Kwan, I., Dickson, K., Richardson, M., MacDowall, W., Burchett, H., Stansfield, C., Brunton, G., Sutcliffe, K., & Thomas, J. (2020). Cyberbullying and children and young people’s mental health: a systematic map of systematic reviews. Cyberpsychology, Behavior, and Social Networking, 23(2), 72–82.


In This Issue

Note from the Editor

Research Articles

Muhammad Faris Abdullah, Mohamad Sahari bin Nordin, Suhailah binti Hussien, Norhayati Mohd. Alwi & Noor Suzilawati binti Rabe
Validation of a Sejahtera Living Index Using the Rasch Model

Fatmir Shehu
Investigating Ismā’īl Rājī al-Fārūqī’s Methodology in the Study of Christianity through Selected Textual Analysis from His Christian Ethics

Mirsad Karić, Šejma Aydin, Huseyin Korkut & Muhidin Mulalić
Paradoxical and Insufficient? Gender Quotas and Placement Mandates in Bosnia and Herzegovina’s 2020 Local Elections

Aida Mokhtar & Faiswal Kasirye
Gestalt and Semiotic Analyses of Brand Communication on Disability Inclusion: The Case of Malaysia and the US

Roy Anthony Rogers, Noraiz Arshad & Iftikhar Ali
Understanding the Decline of Pakistan-US Alliance and the Growing Influence of China in Pakistan

Sarina Yusuf, Misha Teimouri, Muhamad Shamsul Ibrham, Nan Zakiah
Megat Ibrahim, Syahida Mohd Nazri & Stephanie Ann Victor
Let’s Think They are Safe Online! A Malaysian Perspective on The Classification of Children’s Cyber Risks

Farah Fazlinda Mohamad, Khazaila bt Zaini & Nur Syahidatul Idany
Social Media Use for English Learning in Southeast Asia: A Systematic Review

Ali Mehellou, Mohamad Saifudin Mohamad Saleh & Bahiyah Omar
Maqāṣid al-Shari‘ah as Goal Framing for Sustainable Behaviours: A Conceptual Framework

Siti Aeisha Joharry
Faith in The Time of Coronavirus: A Corpus-assisted Discourse Analysis

Abdul Manan Ismail, Ahmad Syukran Baharuddin & Muhammad Hazim Ahmad
COVID-19: Analysing the Principle and Application of I’tibār Ma’ālāt in the Selected Fatwas Issued by the Malaysian National Council for Islamic Religious Affairs (MKI)

Sharifah Nursyahidah Syed Annuar & Muhamad Takiyudin Ismail
The Challenges of Civil Society Organisations: NGO-isation of Resistance in Malaysia?

Anhar Anshory, Ahmad Faizuddin Ramli & Ramli Awang
The Authenticity of Theology in Scientific and Technological Thinking

Research Notes

Alwi Alatas, Agus Setiawan, Achmad Sunjayadi & Yunadi Ramlan
The Seminar on Da‘wah in Kuala Lumpur in 1977 and the Emergence of Hijab Awareness in Indonesia

Book Review

ISSN 0128-4878 (Print)
ISSN 2289-5639 (Online)