INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 13, Issue 14, (2023) E-ISSN: 2222-6990

Cybersecurity Issues among High School Students: A Thematic Review

Intan Diana[1,2], Ismi Arif Ismail[1,2], Mohd Zairul[1,3]

[1]Institut Pengajian Sains Sosial, Universiti Putra Malaysia, [2]Faculty of Educational Studies, Universiti Putra Malaysia, [3]Department of Architecture, Faculty of Design and Architecture, Universiti Putra Malaysia

Corresponding Author's Email: intanabrahman@gmail.com

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v13-i14/12290 DOI:10.6007/IJARBSS/v13-i14/12290

Published Date: 19 August 2023

Abstract

Cybersecurity refers to the methods and technology used to prevent unauthorised access, use, disclosure, interruption, alteration, or the destruction of computer systems, networks, and sensitive information from cyber-attacks. Cyber-attacks are among the most severe issues confronting today's fast-changing technology. Individuals well-versed in cybersecurity can identify, respond to, and limit the impact of cyber threats on them. There have been reports of people being assaulted with cyber threats despite their expertise in cybersecurity. A variety of elements, including individual characteristics, cause this cyber-attack. Therefore, this thematic study aims to emphasise the elements that encourage high school students, to incorporate cybersecurity into their daily life, mainly when using the internet. Aside from that, the elements are referred to avoid cyber-attacks. A list of keywords relevant to the scope of this study is used in two databases, namely Scopus and Science Direct, in which a total of 27 papers were finalised to be reviewed. A thematic review was conducted using ATLAS.ti version 22, the papers were coded, categorised, and themed. The finding revealed four final themes: demographic, psychological, family, and societal elements. The new results have contributed to the unique elements related to cybersecurity issues among high school students. This study benefits future research focusing on aspects that could drive high school students to practice cybersecurity so that they will not become the victims of cyber-predator.

Keywords: Cybersecurity, Cyber-Predator, High School Students, Thematic Review, ATLAS.ti

Introduction

Cybersecurity uses procedures and tools to guard computer networks, systems, and private data against unwanted access, usage, disclosure, interruption, alteration, and destruction (Irfan et al., 2020). This procedure includes safeguarding data's confidentiality, integrity, and availability and protecting against cyber threats like hacking, phishing, malware, and ransomware (Khan et al., 2020). Risk management, incident response, and disaster recovery strategies are also included in cybersecurity. The growing reliance on technology and internet-

connected devices has made cybersecurity a top priority for all stakeholders, including people, corporations, governments, as well as teenagers. According to the International Communication Union (ITU), teenagers are the group of people with a high percentage who use the internet globally which indicated more than 70% (ITU, 2021). Also, according to the National Centre for Missing and Exploited Children (NCMEC, 2023), the website reported an increment of online enticement among children from 2019 to 2020 is 97.5%. The growing number of these reports raises concerns that must be addressed. Typically, teenagers are among high school students.

In high school, cybersecurity refers to the precautions taken to guard against unauthorised access to, use of, disclosure of, disruption of, alteration of, or destruction of sensitive information and systems (Martínez-Domínguez & Fierros-González, 2022). This term can involve protecting the computer networks and devices from online threats like malware, phishing, and hacking and maintaining the privacy, accuracy, and accessibility of data stored on these systems (Khan et al., 2020). High school students may receive cybersecurity education through seminars, workshops, or other educational initiatives (Rahman et al., 2020). They may be advised on the value of using strong passwords, performing frequent backups and updates, and exercising caution when disclosing personal information online. However, studies showed that students have to face varieties of cyber threats like cyber-exploitation, cyber-attack, and cyberbully. This thematic review paper highlight aims to identify the elements that can motivate high school students to practice cybersecurity so that they will able to avoid being attacked by cybercriminals or individuals who have malicious intent on them through cyberspace. Therefore, the following research question is being addressed in this study:

Research Question: What are the elements related to cybersecurity issues among high school students discussed in the literature from 2018 to 2023?

Materials and Methods

The phrase "thematic review" is used since this research technique employs procedural thematic analysis in the literature review, first established by (Zairul, 2020; Zairul, 2021). According to Clarke and Braun (2013), thematic analysis detects patterns and develops themes through attentively reading the subject. The next stage is to discover elements related to cybersecurity concerns among high school students in the most recent publications from 2018 to 2023. The research principle is to examine and interpret the findings to identify elements that could cause high school students to practice cybersecurity.

The literature is chosen using a variety of elements, including 1) publications between 2018 and 2023, 2) Containing at least one keyword, such as cybersecurity and high school students and 3) Concentrating on aspects of high school students in cyberspace. The decision is not to limit certain countries in defining the elements associated with cybersecurity issues.

Scopus and Science Direct databases were used to find relevant literature. The initial search yielded 71 articles from (SCOPUS) and 56 items from (Science Direct). However, 100 articles were eliminated due to premature and anecdotal results or because they did not discuss cybersecurity issues among high school students. Some reports were incomplete or inaccessible, with broken and overlapping links and inadequate metadata. As a result, the final document will be reviewed for up to 27 articles (Refer to Table 1).

The articles were uploaded as primary documents into ATLAS.ti 22, and then each paper was categorised as 1) author; 2) issue number; 3) periodic; 4) publisher; 5) volume; and 6) year of publication. As a result, articles may be studied based on the year they were published and what the debate trend is based on the year. ATLAS.ti 22 has 27 articles that have been finalised into the final document (See Figure 1).

Table 1
Search strings from Scopus and Science Direct databases.

SCOPUS	1. *TITLE-ABS-KEY (cybersecurity* 2. *AND high school students) AND* 3. *PUBYEAR > 2018 AND PUBYEAR > 2023*	71 results
Science Direct	cybersecurity AND high school students	56 results
	Total	**127 results**

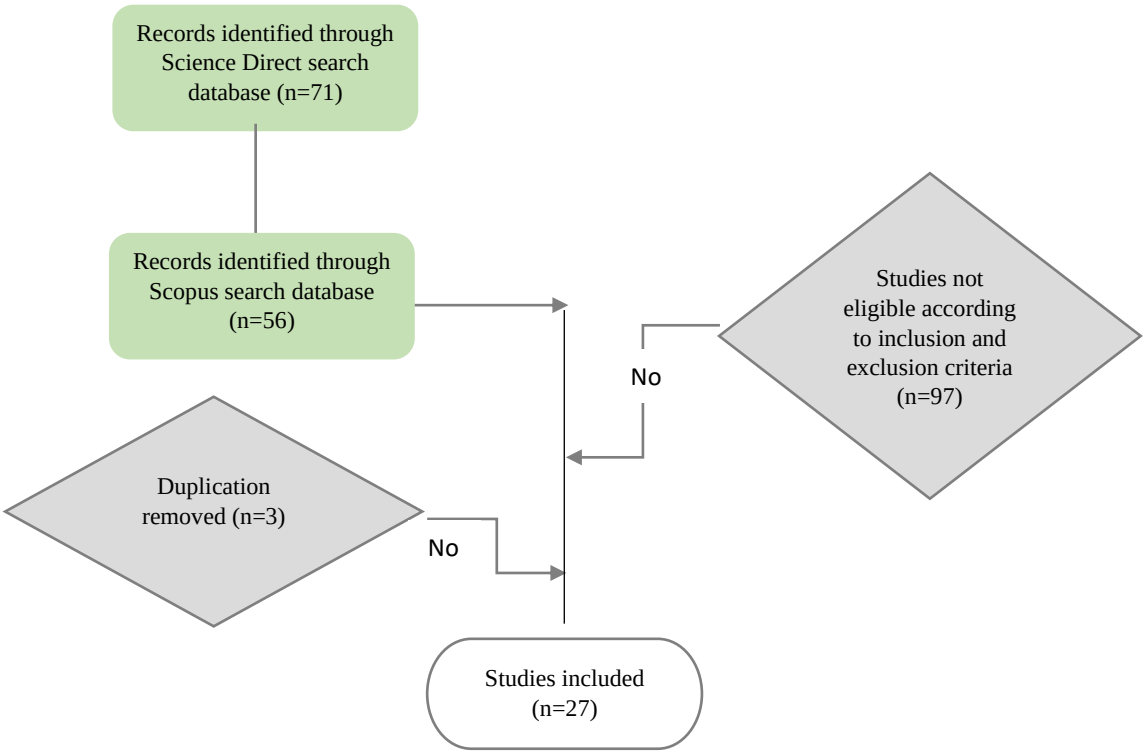

Figure 1: Inclusion and exclusion criteria in the thematic review.

The remaining 27 metadata were copied to ATLAS.ti 22 and made into primary documents. As illustrated in Figure 2, depending on the metadata created in Mendeley, multiple groupings were initiated automatically in the code group. The ATLAS.ti 22 classification has made the organisation much more superficial and orderly. 87 codes were formed during the initial round of coding. The codes were sorted into numerous themes to address the research question, "What are the elements related to cybersecurity among high school students discussed in the literature from 2018 to 2023?" resulting in a final of four primary themes to answer the research question. The findings of this review will be divided into two categories: quantitative results and qualitative findings.

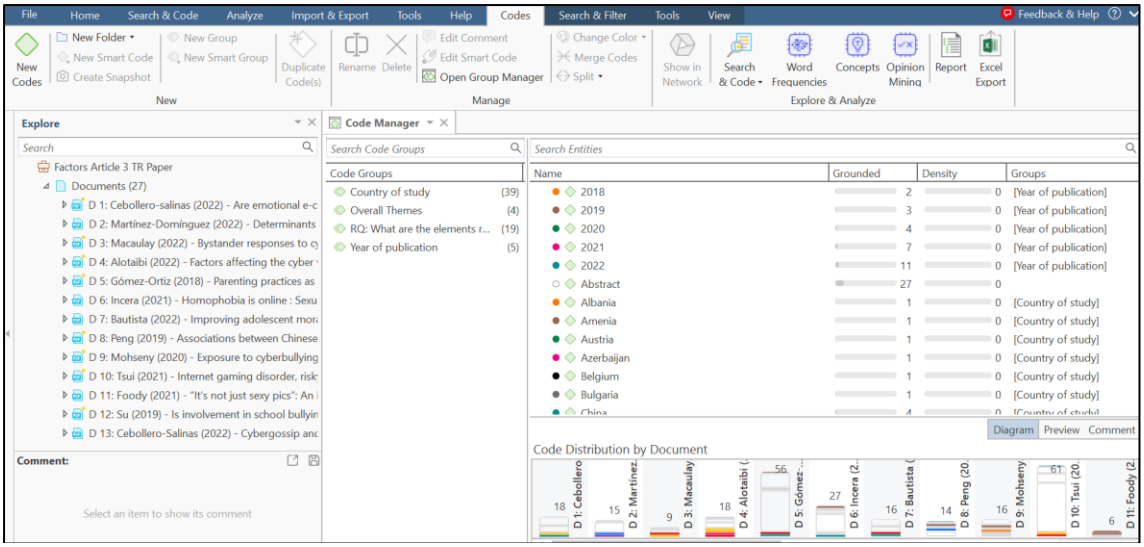

Figure 2: Mendeley metadata is used to create the code group.

Results and Discussions

Quantitative Results

This section summarises the key findings of the thematic review. According to Table 2, the trend of publishing is increasing from year to year, except for 2023, when the direction indicates that publishing is gradually diminishing, resulting in zero publications. It is because 2023 is still in the early year of January. Table 1 lists publications discovered by journal and year. The journals' titles are Computers and Education, Telecommunications Policy, Computers in Human Behavior, Technology in Society, MDPI, BMC Psychiatry, Psychiatry, and Behavioral Sciences, Frontiers in Psychiatry, Children and Youth Services Review, Journal of Educational and Social Research, Children and Youth Services Review, Comprehensive Psychiatry, Computers, and Education, Computers in Human Behavior. The most publication published is regarding Computers in Human Behavior, with ten publications in total.

Table 2
Publications found according to journal and year.

No	Journal	2018	2019	2020	2021	2022	2023	Total
1	Computers & Education	-	-	-	-	2	-	2
2	Telecommunications Policy	-	-	-	-	1	-	1
3	Computers in Human Behavior	-	-	1	4	5	-	10
4	Technology in Society	-	-	-	-	1	-	1
5	MDPI	1	-	-	1	-	-	2
6	BMC Psychiatry	-	2	-	-	-	-	2
7	Psychiatry and Behavioral Sciences	-	-	1	-	-	-	1
8	Frontiers in Psychiatry	-	-	-	1	-	-	1
9	Children and Youth Services Review	-	1	1	-	1	-	3
10	Journal of Educational and Social Research	-	-	1	-	-	-	1
11	Teaching and Teacher Education	-	-	-	1	-	-	1
12	Journal of Adolescent Health	-	-	-	-	1	-	1
13	Journal of Psychosocial Research on Cyberspace	1	-	-	-	-	-	1
	Total	2	3	4	7	11	0	27

The 27 research publications were examined for similarities and differences using comparisons among the articles. The process is carried out to ensure uniformity in the outcome of the subcategories. A list of publications is provided in Table 1, along with a breakdown of each publication's subcategory. Additionally, numerous sources related to cybersecurity issues have been discovered. The phrases used to portray elements related to cybersecurity issues among high school students have been utilised to categorise the research publications into themes. Four main themes are identified from the original coding of 87 codes: demographic element, psychological element, family element, and societal element. The four themes from Table 3 are displayed.

Table 3
The themes according to year.

	2018	2019	2020	2021	2022	2023	Total
Demographic element	1	4	7	3	2	-	17
Psychological element	-	-	1	2	4	-	7
Family element	-	2	4	3	3	-	12
Societal element	2	1	4	2	7	-	16

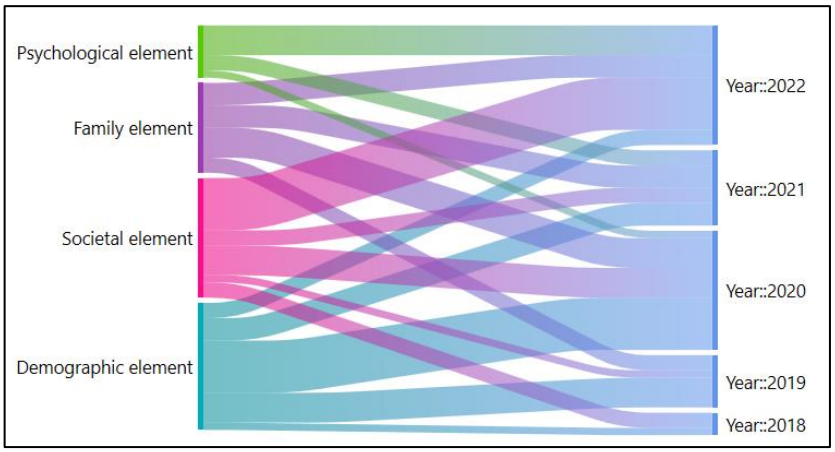

Figure 3: Sankey Diagram on the four themes that correlate with the year of publication.

Table 4
Author versus themes.

No	Author / Theme	Demographic element	Psychological element	Family element	Societal element
1	(Cebollero-Salinas, Orejudo, et al., 2022)			/	
2	(Martínez-Domínguez & Fierros-González, 2022)	/			
3	(Macaulay et al., 2022)				/
4	(Alotaibi & Mukred, 2022)			/	/
5	(Gómez-Ortiz et al., 2018)		/		/
6	(Incera et al., 2021)		/		
7	(Bautista et al., 2022)				/
8	(Peng et al., 2019)	/	/		
9	(Mohseny et al., 2021)		/		
10	(Tsui & Cheng, 2021)			/	/
11	(Foody et al., 2021)		/		
12	(Su et al., 2019)				/
13	(Cebollero-Salinas, Orejudo, et al., 2022)	/			
14	(Kim & Faith, 2020)		/		
15	(Kallciu et al., 2020)	/	/	/	/
16	(Sciacca et al., 2021)				/
17	(Li et al., 2019)	/	/		
18	(Cosma et al., 2022)		/		
19	(Schiks et al., 2022)		/		
20	(Bullo & Schulz, 2022)	/			/
21	(Knauf et al., 2018)				/
22	(Steer et al., 2020)		/		/
23	(Calvete et al., 2022)				/
24	(Bleize et al., 2021)			/	
25	(Rakic et al., 2021)	/	/		
26	(Boer et al., 2021)	/			
27	(Pichel et al., 2022)			/	

The patterns were analysed using the year of the study conducted versus themes, as shown in Table 3 and Figure 3. The paper found the elements in the demographic and societal that had begun in 2018, and no article discussed the psychological and family elements in 2018. In addition, demographic and societal elements were the two most popular themes in 17 and 16 publications, respectively, as indicated in Table 3. Figure 4 demonstrates the most popular year discussing psychological elements is 2022, which are 11 papers. Table 4, author versus themes, indicates that Kallciu et al (2020) stated all the four final themes.

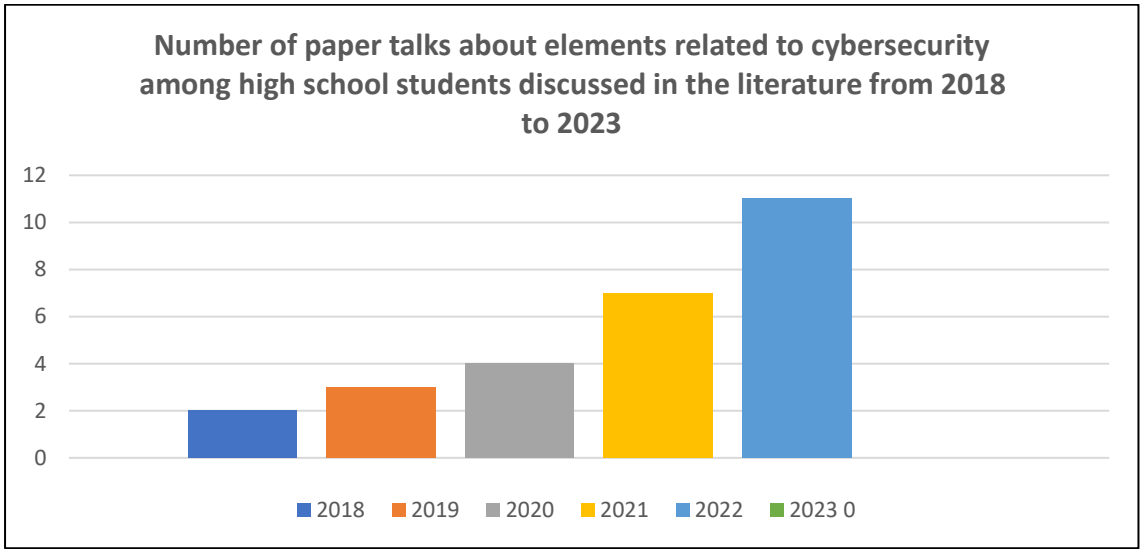

Figure 4: Number of publications versus the year.

The word cloud in Figure 5 shows that bullying and cyberbullying were the two most frequently used terms across 27 articles. Then, in Figure 5, it was possible to locate and reference the phrases school, internet, social, study, adolescents, and other words.

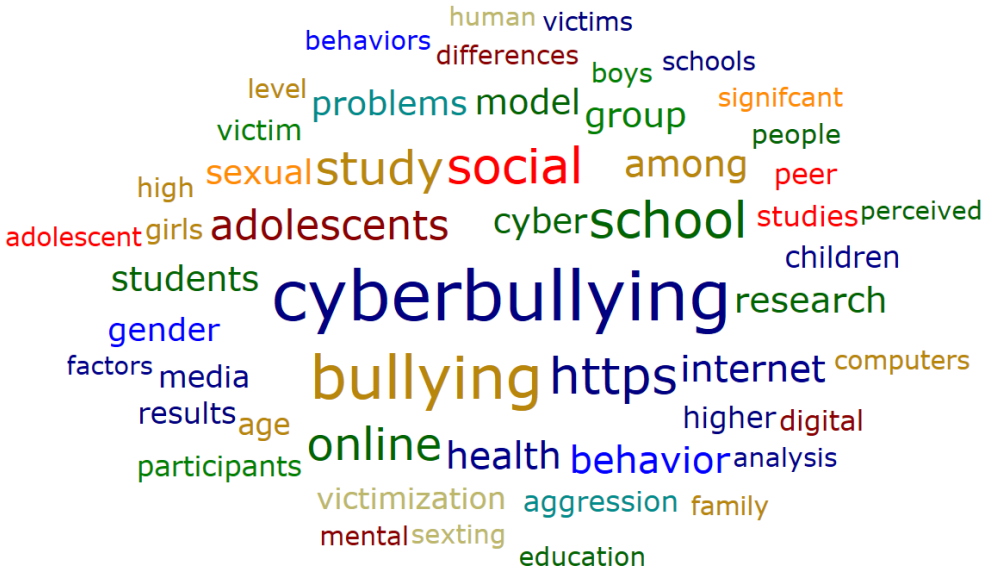

Figure 5: Word Cloud generated from 27 articles.

The results of this study indicate an upward trend in 2022, that are, 40 publications. Results indicate that eight articles are the most frequently discussed nation regarding cyber danger, followed by China and the Netherlands, each with four publications. The United States of America (USA), with four periodicals, has the third-highest number of publications nationwide. Australia, Netherlands, and Switzerland are other nations; the latter had two publications. Bangladesh, England, Georgia, Hungary, Iran, Ireland, Mexico, Saudi Arabia, Turkey, the United Kingdom, and Vietnam are the following countries, each with one publication. Nevertheless, Table 5 and Figure 6 provide evidence that no study on cybersecurity among high school students has been conducted in Malaysia.

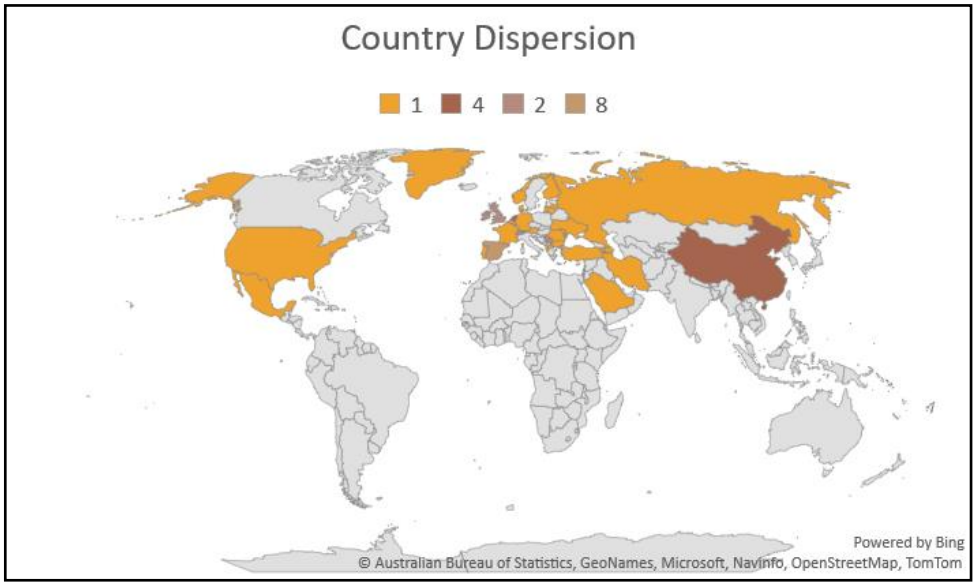

Figure 6: Articles based on the country published.

Table 5
The distribution of articles according to country and year.

No	Country/Year	2018	2019	2020	2021	2022	2023	Total
1	Albania	-	-	1	-	-	-	1
2	Amenia	-	-	-	-	1	-	1
3	Austria	-	-	-	-	1	-	1
4	Azerbaijan	-	-	-	-	1	-	1
5	Belgium	-	-	-	-	1	-	1
6	Bulgaria	-	-	-	-	1	-	1
7	China	-	3	-	1	-	-	4
8	Denmark	-	-	-	-	1	-	1
9	England	-	-	-	-	1	-	1
10	Finland	-	-	-	-	1	-	1
11	France	-	-	-	-	1	-	1
12	Germany	1	-	-	-	-	-	1
13	Greenland	-	-	-	-	1	-	1
14	Iran	-	-	1	-	-	-	1
15	Ireland	-	-	-	2	-	-	2
16	Israel	-	-	-	-	1	-	1
17	Kazakhstan	-	-	-	-	1	-	1
18	Latvia	-	-	-	-	1	-	1

19	Lithuania	-	-	-	-	1	-	1
20	Luxembourg	-	-	-	-	1	-	1
21	Malta	-	-	-	-	1	-	1
22	Mexico	-	-	-	-	1	-	1
23	Moldova	-	-	-	-	1	-	1
24	Netherlands	-	-	-	2	2	-	4
25	North Macedonia	-	-	-	-	1	-	1
26	Norway	-	-	-	-	1	-	1
27	Portugal	-	-	-	-	1	-	1
28	Romania	-	-	-	-	1	-	1
29	Russia	-	-	-	-	1	-	1
30	Saudi Arabia	-	-	-	-	1	-	1
31	Scotland	-	-	-	-	1	-	1
32	Serbia	-	-	-	1	1	-	2
33	Spain	1	-	-	1	6	-	8
34	Switzerland	-	-	-	-	2	-	2
35	Turkey	-	-	-	-	1	-	1
36	Ukraine	-	-	-	-	1	-	1
37	United Kingdom	-	-	1	-	1	-	2
38	USA	-	-	1	-	-	-	1
39	Wales	-	-	-	-	1	-	1
	Total	2	3	4	7	40	0	56

Qualitative Findings

Figure 6 and Figure 7 portray network diagrams containing four themes extracted from the 27 articles: Demographic element, Psychological element, Family element, and Societal element.

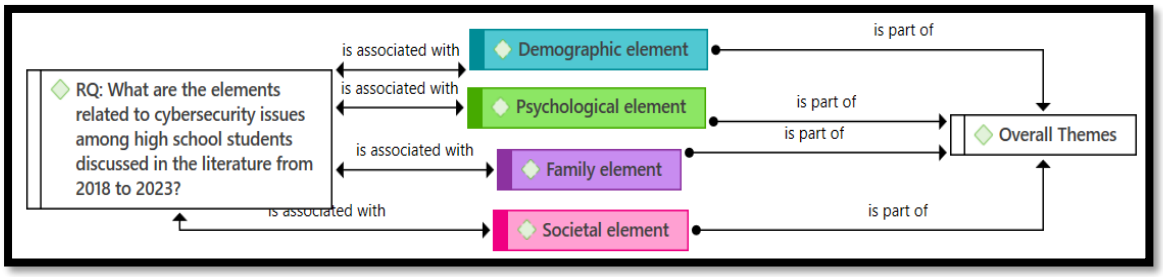

Figure 6: A network of the four themes.

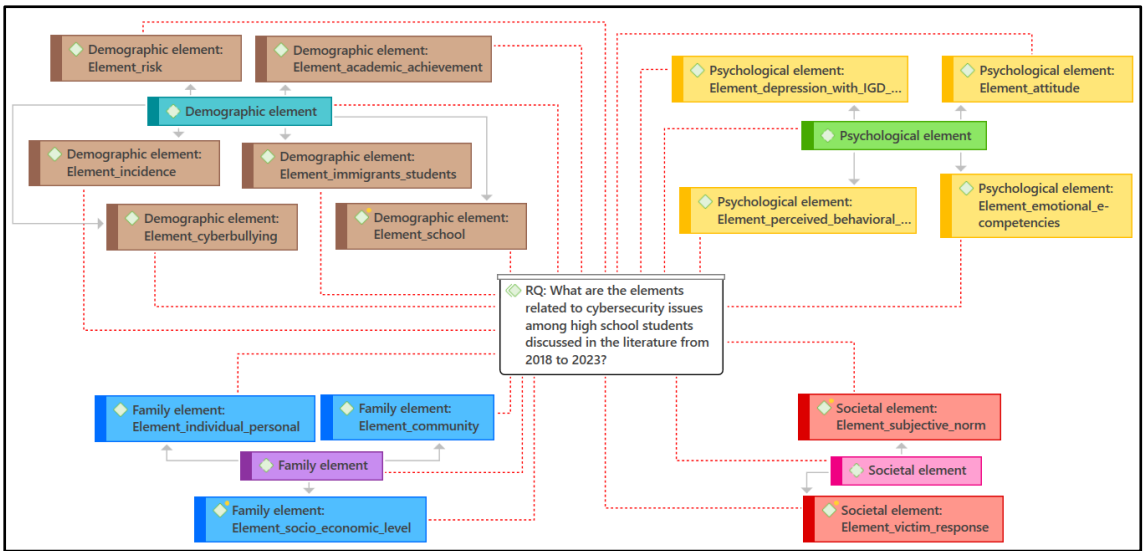

Figure 7: An overall network of how thematic reviews are used to answer the Research Question.

Research Question: What are the elements related to cybersecurity issues among high school students discussed in the literature from 2018 to 2023?
In the first round, the coding resulted in a demographic element.

Theme 1: Demographic element
People are vulnerable to cyber threats because they rely on the internet for most of their daily activities. Therefore, they must engage in online cybersecurity training to protect themselves from future cyber-attacks. Numerous factors can encourage someone to practise cybersecurity to avoid becoming a cyber-victim. One of the reasons is due to demographic elements. Demographic elements are features of a population that are used to characterise and classify groups of people. These characteristics can include age, gender, race, ethnicity, income, educational level, type of school, occupation, and location. Demographic data is frequently utilised in market research, public policy, and other sectors to understand better and put a target on specific groups of individuals.

From the 27 articles, Mohseny et al (2021) found that boys are more prone to cyberbullying and cyber victimisation than girls. It is because boys are usually braver compared to girls, so they have the character to fight each other whenever they can. To support this, according to Foody et al. (2021), sexting behaviour, which is one of the cyber behaviour, is more prone by the boys, too, for two-way sexting. Sexting means sending sex messages, including sexy pictures, to the receivers or victims. The same gender is also supported by Cosma et al (2022) when they revealed that boys tend to cyberbully others rather than girls. This research was done in 46 countries, meaning there was a diversity of locations worldwide.

The male gender, attending boarding school and having poor relationship with parents also related to the characteristics of being a victim or cyberbullying perpetrator (Li et al., 2019). Other than that, Kim & Faith (2020) mentioned that immigrant youths who frequently use ICT for leisure have more tendency to be cyberbullying victims. Unfortunately, cyber-victims' consequences are they tend to face headaches and sleep problems. Surprisingly, Schiks et al. (2022) discovered that cybercriminals in high technology have high IQs compared to ordinary

criminals. This situation showed that the more advanced technology is, the more complex protection should be applied to the technology. However, the demographic element discussion in the current studies is minimal; thus, this situation lacks argument on demographics and how it relates to cybersecurity. Figure 8 shows a network diagram regarding the Demographic element theme.

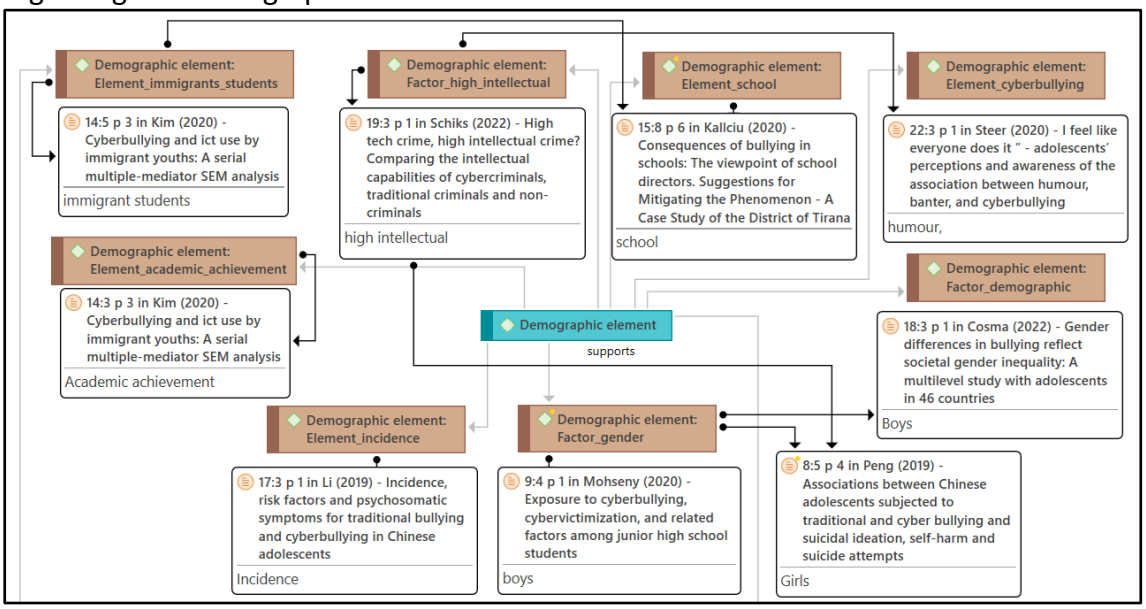

Figure 8: Network diagram from ATLAS.ti 22 about the Demographic element.

In the second round, the initial coding resulted in a psychological element.

Theme 2: Psychological element

A psychological element can be defined as an aspect of the mind or mental processes that contribute to a person's overall psychological function. These elements involve feelings, thought processes, behaviour and personality traits, and a person's psychological composition results from interactions and mutual influences. The psychological element in this research context is defined as a risk factor that enhances the likelihood of children and adolescents becoming cyber-victims or attacking their peers via Information, Communication and Technology (Gómez-Ortiz et al., 2018).

Many psychological elements motivate high school students to practice cybersecurity or aspects to avoid cybercrime. Some of the examples that can encourage people to practice cybersecurity are emotional e-competencies (Cebollero-Salinas, Cano-Escoriaza, et al., 2022). In comparison, some psychological element that drives someone to involve with cybercrime is behavioural intention towards cyber violence (Alotaibi & Mukred, 2022). Incera et al. (2021) found that sexual minorities such as bisexual, homosexual, asexual, or queer adolescents experienced online sexual orientation discrimination during online. Those who did sexting tend to have mental health outcomes like depression and anxiety.

Consequently, high school students who were cyber-victims tend to have suicidal ideation, self-harm and suicide attempts which are very dangerous (Peng et al., 2019). To support this, Boer et al (2021); Tsui & Cheng (2021) said that internet gaming disorder, high-intensity use of social media and risky online behaviour also could cause mental health. Recently, Pichel et al (2022) told that students who are addicted to alcohol would tend to be cyberbully

perpetrators. The most important thing is that the accountability increment in messaging apps should be emphasised to help reduce cyber aggression (Bleize et al., 2021). Nevertheless, the psychological element is rarely discussed in cybersecurity, providing a gap in establishing students' psychological elements related to cybersecurity practices. Figure 9 indicates a network diagram regarding the Psychological element theme.

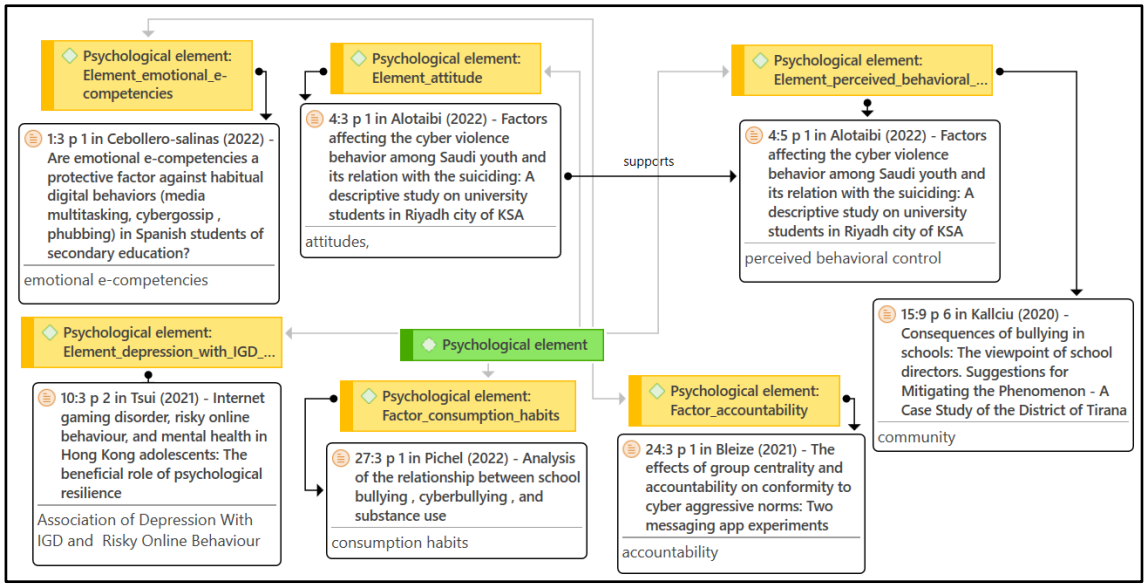

Figure 9: Network diagram from ATLAS.ti 22 about the theme of the Psychological element.

In the third round, the coding resulted in a family element.

Theme 3: Family element

The family element refers to a family unit's traits, relationships, and dynamics (Gómez-Ortiz et al., 2018). It covers things like family cohesion and functions overall, communication styles, roles and obligations of family members, and financial and emotional support (Rakic et al., 2021). The influence of one's family can have a significant impact on how one behaves, feels, and makes decisions. It may also impact a person's physical and emotional well-being and the capacity to handle stress and difficulties.

Martínez-Domínguez & Fierros-González (2022) explains that internet usage permitted by family, especially the parents, can cause someone to be involved in a cyber-attack when they are online. While children's pattern of using the internet depends on their level of schooling, economic status, digital skills, and place of residence. It includes the presence of electronic devices and infomediaries in the household.

Gómez-Ortiz et al (2018) said parenting in the family could be the preventive element for high school students to be involved with cyberbullying. According to Kallciu et al. (2020), a family's economic status situation could be the element in the emergence of bullying. In addition, Rakic et al (2021) informed that family characteristics such as the family's affluence status, the father's occupation, communication with the father, and the family's support could be the factors that could help raise awareness in getting rid of cyberbully. Nevertheless, the lack of family element discussion regarding programs involved with children at school is the cause to

have a strategy to help high school students practice cybersecurity online. Figure 10 reveals a network diagram regarding the Family element theme.

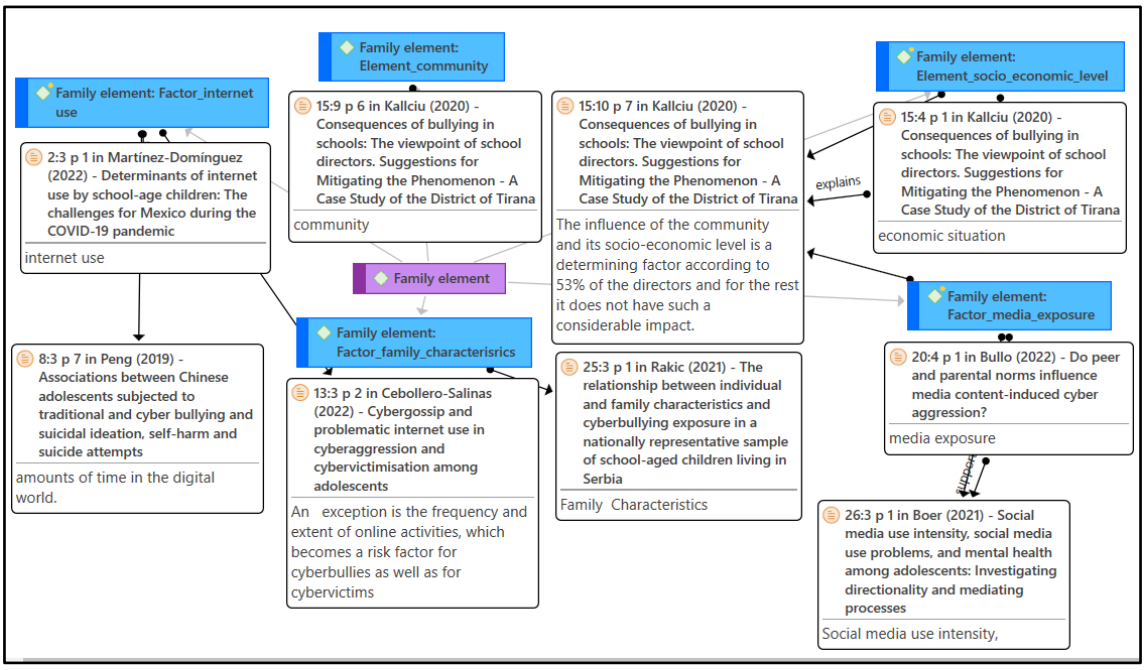

Figure 10: Network diagram from ATLAS.ti 22 about the Family element.

In the fourth round, the coding resulted in a societal element.

Theme 4: Societal Element

The cultural, economic, political, and social forces that shape and give impact to the operation of society are referred to as societal elements. These factors include the economy, governance, education, healthcare, religion, and societal norms and values. Individuals and groups within a society can be affected by societal aspects, which can also differ between communities. Understanding societal aspects are essential for comprehending and interpreting a society's social, economic, and political setting.

According to Macaulay et al (2022), victim response is the main element for a bystander responding to cyberbullying. It implies that the more upset a cyberbullying victim is, the more concern a bystander will have for the victim. On the other hand, Bautista et al (2022) explained that Collective Intelligence (CI) is part of the societal element. CI is a group of responses to help to increase an individual's morale. Morality is essential for a person's life to live in harmony, including cyberspace. Su et al (2019) said that homicidal ideation and behaviours are a societal element. In addition, cyber gossip and problematic internet use are also part of the social element that can enhance students' involvement with cyber problems (Cebollero-Salinas & Orejudo et al., 2022). Teenagers will experience cyberaggression and victimisation if they are not cautious when using the internet.

Bullo and Schulz (2022) portrayed that parental norms influence media content-induced cyber aggression. On the other hand, Knauf et al (2018) cited the context of cyberbullying for bystanders' social-cognitive and affective reactions. Calvete et al (2022) stressed that online peer victimisation teenagers have high risk of emotional problems. Perhaps some people

assume humour and banter are common in cyberbullying behaviour (Steer et al., 2020). This incident demonstrated how poorly people understand other people's emotions. Nonetheless, societal element among neighbours is rarely discussed in cybersecurity, providing a gap in establishing students' societal part to practice cybersecurity when using the internet. Figure 11 indicates a network diagram regarding the Societal element theme.

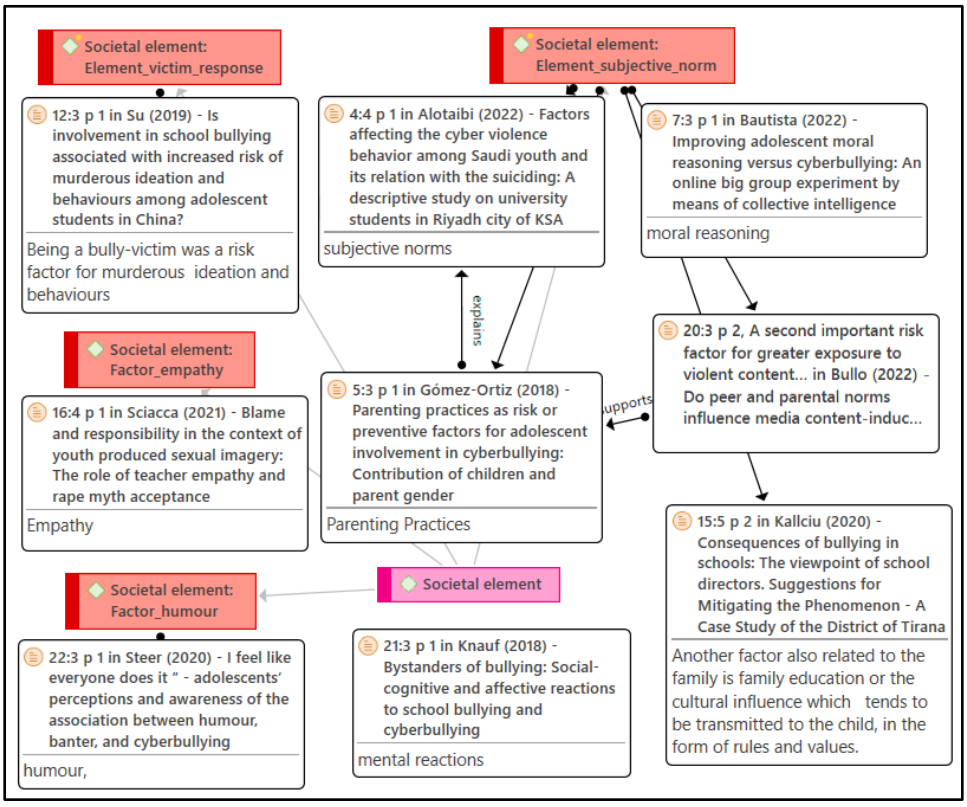

Figure 11: Network diagram from ATLAS.ti 22 about the Societal element.

Conclusion and Future Study

This review paper highlights demographic, psychological, family, and societal themes associated with cybersecurity issues among high school students. Despite the details being discussed, several issues are raised. Some parts include the psychological aspect, which is rarely addressed in cybersecurity education, leaving a gap in determining how high school students' cybersecurity awareness could be increased in an online environment. Furthermore, the demographic element in the current studio is lacking in terms of academic discussion, with very few articles mentioning how a specific demographic influences student to practice cybersecurity in the cyber sphere.

Additionally, the inability to discuss family issues has hampered efforts to address cyber-attack issues among high school students and exacerbated psychological problems. Further, the societal component of cybersecurity issues will aid in lowering student cyber risk. To sum up, future research should recommend a set of guidelines on how to produce the best practices of cybersecurity among society—specifically high school students by referring to the four elements discussed in this paper. This is to solve cyber threats attack and improve people's quality of life. In conclusion, this study offers the aspects related to cybersecurity that

can be used as a guide by the public or private sectors to address the various types of cyber-attacks that are becoming more common in most countries.

Acknowledgement
Appreciation to the Malaysian Ministry of Education awarded the *Hadiah Latihan Persekutuan* (Industrial Revolution 4.0) scholarship to finance one of the authors' study leave.

References

Alotaibi, N. B., & Mukred, M. (2022). Factors affecting the cyber violence behavior among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA. *Technology in Society*, *68*(January), 101863. https://doi.org/10.1016/j.techsoc.2022.101863

Bautista, P., Cano-escoriaza, J., Sanchez, E. V., Cebollero-Salinas, A., & Orejudo, S. (2022). Improving adolescent moral reasoning versus cyberbullying: An online big group experiment by means of collective intelligence. *Computers & Education*, *189*, 1–12. https://doi.org/10.1016/j.compedu.2022.104594

Bleize, D. N. M., Anschutz, D. J., Tanis, M., & Buijzen, M. (2021). The effects of group centrality and accountability on conformity to cyber aggressive norms: Two messaging app experiments. *Computers in Human Behavior Journal*, *120*(January). https://doi.org/10.1016/j.chb.2021.106754

Boer, M., Stevens, G. W. J. M. J. M., Finkenauer, C., de Looze, M. E., van den Eijnden, R. J. J. M., Looze, M. E. De, Regina, J. J., & Eijnden, M. Van Den. (2021). Social media use intensity, social media use problems, and mental health among adolescents: Investigating directionality and mediating processes. *Computers in Human Behavior*, *116*(November 2020), 1–17. https://doi.org/10.1016/j.chb.2020.106645

Bullo, A., & Schulz, P. J. (2022). Do peer and parental norms influence media content-induced cyber aggression? *Computers in Human Behavior*, *129*(December 2021), 1–12. https://doi.org/10.1016/j.chb.2021.107136

Calvete, E., Orue, I., Echezarraga, A., Cortazar, N., Fern, L., & Fernández-González, L. (2022). A growth mindset intervention to promote resilience against online peer victimization: A randomized controlled trial. *Computers in Human Behavior*, *135*(June), 107373. https://doi.org/10.1016/j.chb.2022.107373

Cebollero-Salinas, A., Cano-escoriaza, J., & Orejudo, S. (2022). Are emotional e-competencies a protective factor against habitual digital behaviors (media multitasking, cybergossip, phubbing) in Spanish students of secondary education? *Computers and Education*, *181*(January), 1–13. https://doi.org/10.1016/j.compedu.2022.104464

Cebollero-Salinas, A., Orejudo, S., Cano-Escoriaza, J., Iniguez-Berrozpe, T., & Íñiguez-Berrozpe, T. (2022). Cybergossip and problematic internet use in cyberaggression and cybervictimisation among adolescents. *Computers in Human Behavior*, *131*, 1–11. https://doi.org/10.1016/j.chb.2022.107230

Cosma, A., Bjereld, Y., Elgar, F. J., Richardson, C., Bilz, L., Craig, W., Augustine, L., Molcho, M., Malinowska-Cieslik, M., & Walsh, S. D. (2022). Gender differences in bullying reflect societal gender inequality: A multilevel study with adolescents in 46 countries. *Journal of Adolescent Health*, 1–8. https://doi.org/10.1016/j.jadohealth.2022.05.015

Foody, M. M., Mazzone, A., Laffan, D. A., Loftsson, M., O'Higgins Norman, J., & Higgins, J. O. (2021). "It's not just sexy pics": An investigation into sexting behaviour and behavioural problems in adolescents. *Computers in Human Behavior*, *117*(May 2020), 1–8.

https://doi.org/10.1016/j.chb.2020.106662

Gómez-Ortiz, O., Romera, E. M., Ortega-Ruiz, R., & Del Rey, R. (2018). Parenting practices as risk or preventive factors for adolescent involvement in cyberbullying: Contribution of children and parent gender. *International Journal of Environmental Research and Public Health*, *15*(12), 2664. https://doi.org/10.3390/ijerph15122664

Incera, D., Manuel, G., Gámez-Guadix, M., & Incera, D. (2021). Homophobia is online: Sexual victimization and risks on the internet and mental health among bisexual, homosexual, pansexual, asexual, and queer adolescents. *Computers in Human Behavior*, *119*, 1–10. https://doi.org/10.1016/j.chb.2021.106728

Irfan, H., Akhter, K. J., & Shakeel, R. (2020). Cybersecurity and Multidisciplinary Students: A Survey. *International Journal of Science and Engineering Research*, *11*(4), 1786–1791. https://www.researchgate.net/publication/341255532%0ACybersecurity

ITU. (2021). Measuring digital development: Facts and figures. In *ITU Publications*. https://www.itu.int/en/mediacentre/Documents/MediaRelations/ITU Facts and Figures 2019 - Embargoed 5 November 1200 CET.pdf

Kallciu, N., Noti, K., & Borufi, X. (2020). Consequences of bullying in schools: The viewpoint of school directors. Suggestions for Mitigating the Phenomenon - A Case Study of the District of Tirana. *Journal of Educational and Social Research*, *10*(5), 131–138. https://doi.org/10.36941/jesr-2020-0094

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid covid-19 pandemic. *TechRxiv Powered by IEEE*. https://doi.org/https://doi.org/10.36227/techrxiv.12264722.v1

Kim, S., & Faith, M. S. (2020). Cyberbullying and ICT use by immigrant youths: A serial multiple-mediator SEM analysis. *Children and Youth Services Review*, *110*(July 2019), 1–11. https://doi.org/10.1016/j.childyouth.2019.104621

Knauf, R.-K., Eschenbeck, H., & Hock, M. (2018). Bystanders of bullying: Social-cognitive and affective reactions to school bullying and cyberbullying. *Journal of Psychosocial Research on Cyberspace*, *12*(4). https://doi.org/http://dx.doi.org/10.5817/CP2018-4-3

Li, J., Mahamadou, A., Shen, X., Hesketh, T., Sidibe, A. M., Shen, X., Hesketh, T., Mahamadou, A., Shen, X., Hesketh, T., Sidibe, A. M., Shen, X., & Hesketh, T. (2019). Incidence, risk factors and psychosomatic symptoms for traditional bullying and cyberbullying in Chinese adolescents. *Children and Youth Services Review*, *107*(July), 104511. https://doi.org/10.1016/j.childyouth.2019.104511

Macaulay, P. J. R. R., Betts, L. R., Stiller, J., & Kellezi, B. (2022). Bystander responses to cyberbullying: The role of perceived severity, publicity, anonymity, type of cyberbullying, and victim response. *Computers in Human Behavior*, *131*(January), 1–13. https://doi.org/10.1016/j.chb.2022.107238

Martínez-Domínguez, M., & Fierros-González, I. (2022). Determinants of internet use by school-age children: The challenges for Mexico during the COVID-19 pandemic. *Telecommunications Policy*, *46*(1), 2–18. https://doi.org/10.1016/j.telpol.2021.102241

Mohseny, M., Zamani, Z., Basti, S., Sohrabi, M.-R., Najafi, A., & Tajdini, F. (2021). Exposure to cyberbullying, cybervictimization, and related factors among junior high school students. *Iranian Journal of Psychiatry and Behavioral Sciences*, *14*(4). https://doi.org/10.5812/ijpbs.99357

NCMEC. (2023). *National Centre for Missing and Exploited Children*. Department of Justice. https://www.missingkids.org/theissues/onlineenticement

Peng, Z., Klomek, A. B., Li, L., Su, X., Sillanmäki, L., Chudal, R., & Sourander, A. (2019).

Associations between Chinese adolescents subjected to traditional and cyber bullying and suicidal ideation, self-harm and suicide attempts. *BMC Psychiatry*, *19*(1). https://doi.org/10.1186/s12888-019-2319-9

Pichel, R., Feijoo, S., Isorna, M., Varela, J., Rial, A., Feijóo, S., Isorna, M., Varela, J., & Rial, A. (2022). Analysis of the relationship between school bullying, cyberbullying, and substance use. *Children and Youth Services Review*, *134*(May 2021), 1–8. https://doi.org/10.1016/j.childyouth.2022.106369

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5). https://doi.org/10.18178/ijiet.2020.10.5.1393

Rakic, L., Santric-milicevic, M., Nikolic, D., Vasic, M., & Babic, U. (2021). The relationship between individual and family characteristics and cyberbullying exposure in a nationally representative sample of school-aged children living in Serbia. *International Journal of Environmental Research and Public Health*, 1–23. https://doi.org/https://doi.org/10.3390/ijerph18147443

Schiks, J. A. M. M., Weijer, S. G. A. Van De, Leukfeldt, E. R., van de Weijer, S. G. A., Leukfeldt, E. R., Weijer, S. G. A. Van De, & Leukfeldt, E. R. (2022). High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals. *Computers in Human Behavior*, *126*, 106985. https://doi.org/10.1016/j.chb.2021.106985

Sciacca, B., Mazzone, A., & Norman, J. O. H. (2021). Blame and responsibility in the context of youth produced sexual imagery: The role of teacher empathy and rape myth acceptance. *Teaching and Teacher Education*, *103*, 1–9. https://doi.org/10.1016/j.tate.2021.103354

Steer, O. L., Betts, L. R., Baguley, T., & Binder, J. F. (2020). I feel like everyone does it " - adolescents' perceptions and awareness of the association between humour, banter, and cyberbullying. *Computers in Human Behavior*, *108*, 1–10. https://doi.org/10.1016/j.chb.2020.106297

Su, P.-Y., Wang, G.-F., He, H., Han, A.-Z., Zhang, G.-B., & Xu, N. (2019). Is involvement in school bullying associated with increased risk of murderous ideation and behaviours among adolescent students in China? *BMC Psychiatry*, *19*(1). https://doi.org/10.1186/s12888-019-2108-5

Tsui, Y. Y., & Cheng, C. (2021). Internet gaming disorder, risky online behaviour, and mental health in Hong Kong adolescents: The beneficial role of psychological resilience. *Frontiers in Psychiatry*, *12*, 1–10. https://doi.org/10.3389/fpsyt.2021.722353

Zairul, M. (2020). A thematic review on student-centred learning in the studio education. *Journal of Critical Reviews*, *7*(2), 504–511. https://doi.org/10.31838/jcr.07.02.95

Zairul, M. M. N. (2021). *Ilustrasi ringkas analisa tematik (AT) menggunakan perisian ATLAS.ti 8* (1st ed.). Penerbit Universiti Putra Malaysia.