

# Teachers' Insight: Digital Threats that Imperil Children and Teenagers

Julian Taupe<sup>[0000-0002-9148-835X]</sup>, Verena Knapp<sup>[0009-0005-0982-0472]</sup>, and  
Andreas Bollin<sup>[0000-0003-4031-5982]</sup>

Universität Klagenfurt, Universitätsstraße 65/67, 9020 Klagenfurt am Wörthersee,  
Austria

**Abstract.** As technology becomes increasingly integrated into daily life, the importance of digital security has become a pressing concern. Children in primary and secondary school are especially vulnerable to digital security threats, as they frequently use digital devices for learning and leisure. The number of cybercrime-related crimes has risen in the past decade, while it is not known which threats are most relevant to children and teenagers. To address this issue, this paper reports on a study to identify relevant digital security competencies among young people and prioritize known threats by gathering teacher data. The study classified and prioritized digital security threats and documented the frequency of personal experiences with such threats to establish a basis for future improvements, yielding a structured approach to addressing digital security concerns for pupils. With this knowledge, teachers can understand potential threats children and teenagers have to cope with in their environment and know about missing skills to be acquired through further training. An interesting finding of this study is that a noticeable number of teachers have already experienced incidents of digital threats among pupils, which emphasizes the urgency of dealing with this topic.

**Keywords:** Digital Threats · Research in Informatics Education · Curriculum Gaps · Competencies for Children.

## 1 Introduction

Digital media and technologies are becoming an increasingly important part of society. At the same time, the number of criminal cases people get involved in grows as well [4]. Many threats in the field of digital security also affect the youngest of our society, especially children and teenagers [14]. They face a multitude of threats in this field [6, 7, 11, 12, 14, 16] against which only a few competencies are planned within curricula of primary and secondary school [1, 2, 5, 13]. What is even more complicated about the situation is that children, teenagers and teachers of different generations have grown up with diverse levels of accessibility regarding digital media and technology [8]. Furthermore, it is not known which threats are more relevant to young people than others. For the first time in Austria various digital threats are examined and relevant ones

categorized into four groups. In a study conducted in early 2023, these threats were prioritized by teachers, who also indicated to what extent they have already experienced cases of digital threats among children and teenagers. This data was collected so the following research question can be answered in this paper:

*According to teachers' point of view, what are the major digital threats in the field of digital security children and teenagers have to cope with in Austria?*

Section 2 examines publications and projects on threats and competency transfer in the field of digital security. Section 3 categorizes existing threats in this field. The conducted study is described in section 4, which also includes validity considerations. Section 5 discusses and analyzes the study results. Finally, section 6 presents conclusions and suggests future research directions.

## 2 Related Work

Numerous publications deal with digital risks, threats as well as competencies. In addition, there are various projects and studies in this field.

Eichenberg and Auersperg (2018) address both the opportunities enabled by digital media and technologies as well as the potential risks that arise from their use. The authors define five areas of risks, which they think should be considered in concepts for building media competences: Excessive usage, dysfunctional usage, self-damaging usage, deviant usage, and youth-endangering usage. Furthermore, some threats, characteristics and possible causes are discussed [6].

Various digital risks that children and teenagers are exposed to, including cyberbullying, sexting, sexual harassment and addictive behavior, which can have serious consequences are highlighted by Gasser et al. (2012). Parents, teachers and other adults should actively participate in prevention and intervention to counter these risks. This includes comprehensive education on potential dangers and training in the use of digital media. In addition, various intervention strategies are discussed to support children and teenagers and strengthen their ability to handle digital risks. Overall, a holistic and preventive approach is emphasized to ensure the safety and health of children and teenagers in the digital world [7].

In an article, O'Keeffe and Clarke-Pearson (2011) primarily address the risks posed by social media, including websites such as Facebook or Twitter, virtual worlds like Second Life and media-sharing platforms like YouTube. The focus is on the benefits of using such services and the associated risks, such as cyberbullying or sexting. The approach to addressing these types of risks is suggested to involve the integration of pediatricians [11].

Furthermore, in another article, Tintori et al. (2023) focus on topics such as cyberbullying and grooming. Among other things, it is described how children and teenagers are vulnerable to grooming due to certain factors, such as low self-esteem, lack of social support and insufficient knowledge about the risks of such approaches. Furthermore, the potential impact of grooming on the victim, such as emotional and psychological distress and physical harm, is discussed [16].

With regards to the effects of digital media on the development of children and teenagers, Reid Chassiakos et al. (2016) consider both, opportunities and risks. Although digital media can have positive aspects, they also pose dangers, such as cyberbullying and excessive usage behavior. To minimize these risks, active media education is recommended, which prepares children and teenagers for the safe and responsible use of digital media [12].

The study *EU Kids Online 2020* is a comprehensive study that examines digital risks and opportunities that children and teenagers face in some European countries, whereas Austria was not considered. The study investigates various topics, including cyberbullying, sexting, online addiction, and identity theft. It also highlights how children and teenagers use these technologies to shape and communicate their identities. Recommendations are documented to help improve the awareness of children and teenagers about digital risks and opportunities [14].

The EU initiative in online competence, *Klicksafe*, is coordinated in Germany by the State Center for Media and Communication Rhineland-Palatinate. The initiative aims to teach children, teenagers, parents, and educators how to use digital media safely and competently. The website provides a variety of information and materials on the topic of safety. Topics covered include cyberbullying, sexting, data protection, copyright, and fake news [10].

Furthermore, the *Lehrplan 21* defines the goal of handling media competently and assessing risks correctly. It has been developed between 2010 and 2014. The curriculum distinguishes between competence areas for computer science as well as media and application competence. Many of these are integrated into the individual subject areas and are not explicitly broken down but kept general. For example, competence with the label “Living in the Media Society” is contained, explicitly mentioning a few dangers. These are addressed in the 2<sup>nd</sup> and 3<sup>rd</sup> cycles, which include four school classes of primary school (3 to 6) and three classes of lower secondary school (7 to 9). The *Lehrplan 21* extends continuously over the first school stages, from the elementary stage, through the primary school to the lower secondary school [5, pp. 477-495].

Another example, the curriculum for schools in Berlin and Brandenburg covers classes 1 through 10. This curriculum was introduced in the 2017/18 school year and includes data protection, addiction issues related to digital media, cyberbullying and copyright. By including these topics in the curriculum, students are to be prepared early to handle digital media safely and competently and to meet the challenges associated with their use [13].

In Austria, the so-called *Digital Basic Education* has been introduced as a mandatory subject in the lower secondary school curriculum from the 2022/23 school year. It is based on *DigComp 2.2 AT*, the Austrian version of the European competencies model of the same name. The subject is implemented in classes 5 to 8, with a minimum of one hour per week in the timetable. Within the curriculum, three areas of competencies are defined. These focus on the interaction between media usage and participation in media culture and on developing computational and media-related competencies based on critical thinking, creativity, communication, collaboration, and problem-solving skills [2].

## 2.1 Scope of this Paper

The aforementioned publications, among others, address issues related to digital threats and competencies. However, these publications usually have a specific focus and do not provide a comprehensive overview of all known threats. Furthermore, the detail in describing these threats varies greatly and does not clarify the relevance of respective threats to children and teenagers. To address these issues, this paper provides a comprehensive collection of digital threats in the field of digital security, classified into meaningful and easily understandable categories. Additionally, a study is conducted to determine the threats children and teenagers are mostly confronted with from the perspective of teachers and their experience in that area. In this paper, the term “digital threats” encompasses threats that originate initially or are in any manner encouraged through the use of digital devices and services.

## 3 Background

With this paper we aim to comprehensively examine digital threats for children and teenagers, aiming to build competencies in the future for dominating these. When examining existing publications, it becomes apparent that potential threats and competencies are often discussed separately, although they are closely connected. To approach the objective, various publications are consulted to gather potential threats in the field of digital security. Threats in this realm encompass all threats in a digital context that can harm an individual in any way. These include physical, psychological, social, or material damages. Threats can emerge in any domain involving interfaces or interactions with digital technology, especially within the realm of the internet. The goal is to gather known threats, divide them into simple and comprehensible categories, prioritize them, and document their frequency. To achieve this, teachers from primary and secondary schools are surveyed. They have a unique insight into students’ behavior and serve as a person of trust. Simultaneously, they play a crucial role in future competence development in this field. Examples of known threats in this domain can be divided into the following categories.

### 3.1 Content Harmful to Young People

This category encompasses threats that primarily involve inappropriate content or goods for children or teenagers. Examples include the *exposure to or creation and distribution of illegal content*, as well as *confrontation with inappropriate content* and *purchase of illegal substances online*. These threats revolve around the exposure to or engagement with materials or products that are illegal, harmful, or morally questionable for young people [6, 7, 14].

### 3.2 Social Environment

This category focuses on threats with social interactions that can lead to harmful behaviors, coercion or manipulation with severe emotional, psychological, and

social consequences for children and teenagers. These threats range from *happy slapping* [7] *cyberbullying*, *cyberstalking* to *trivialization of suicide*, *self-harm*, *eating disorders*, etc. [6, 11, 14]. It also includes threats associated with *contact with strangers (online vs. offline)*, which also includes cyber-grooming [4, 16], and *encouragement and instructions for violent or criminal activities* [12]. Regarding cyberbullying, over a third of surveyed teenagers aged 12 to 19 reported having offensive or false information spread about them in private chats at least once. In contrast, only about 7% of respondents indicated that such incidents occurred publicly on the internet [9].

### 3.3 Data, Data Protection & Information

Threats based on information or data are part of this category. It includes threats such as the *misuse of personal information and privacy violations*, *copyright infringements*, *unauthorized access to sensitive data*, *computer or data damage*, *unbalanced or false information*, *information overload* and *reputation damage*. These examples highlight threats associated with the misuse, mishandling or unauthorized access to personal or sensitive information. They can lead to privacy breaches, identity theft, financial loss or reputation damage. Additionally, increasing false or unbalanced information can significantly affect individuals' decision-making processes and beliefs [6, 7, 14]. The frequency of being confronted with such threats increases with age [14].

### 3.4 Online Addiction

This category includes threats that deal with addictive behaviors. They can be divided into *online shopping addiction*, *gaming addiction* and *excessive use of chat forums and social networks* [6, 7]. Online shopping addiction encloses threats with online engagement leading to negative consequences, including excessive online shopping, financial problems, impaired decision-making, and in-app purchases [14]. Some aspects of online shopping may be more relevant to teenagers or adults, but these are nevertheless considered in the study. Gaming addiction refers to the excessive playing of video games. Excessive use of chat forums and social networks refers to prolonged engagement in online communication.

## 4 Study

This report presents the findings of an empirical study examining Austrian teachers' experience with digital security threats for children and teenagers in primary and secondary schools. The study collected data from 708 participating teachers through a survey conducted between April and May 2023. The report analyzes the collected data and discusses the results in the following sections.

#### 4.1 Questionnaire

The survey for this report consisted of three sections. The first section included demographic questions, while the second section explored the teachers' personal use of digital media in the classroom and their engagement with professional development. The third section covered questions about digital security threats as perceived by the teachers and how children and teenagers are exposed to these threats. The survey included closed-ended questions and ranking tasks.

#### 4.2 Population and Sampling

The target population of this study consists of teachers of primary and secondary schools in Austria. As it was not possible to directly sample teachers, the study was conducted through the schools, using a multistage sampling strategy based on the publicly available "School Directory of the Federal Ministry of Education, Science and Research" [3]. The first stage of the sampling involved stratification by federal state, while the second stage involved grouping schools by type. Schools offering both primary and secondary education have been assigned to the matching secondary school group. Within each sub-population, a simple random sampling procedure was used to select schools. The number of schools contacted varied across groups, based on both the potential number of reachable teachers and the experience gained from a previously conducted study in 2022, which indicated varying levels of willingness to participate in the survey among different groups. The sample size of the different school types was determined in such a way that all school types are represented as adequately as possible, while optimizing response rates.

#### 4.3 Distribution

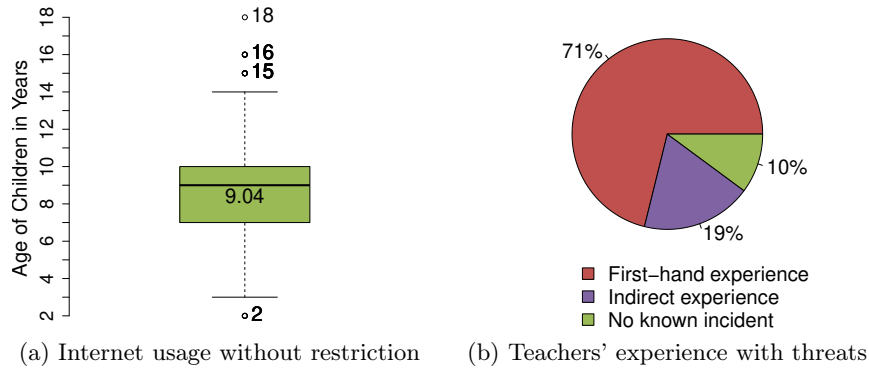
The distribution of the questionnaire for this study followed different procedures due to regional regulations. In the federal states of Carinthia, Tyrol and Vorarlberg, no approval was required from the education directorate for surveying teachers. In Styria and Upper Austria, a simple approval procedure was followed, involving a review of the questionnaire. In Burgenland, Lower Austria and Salzburg, non-binding consent from school directors was obtained before obtaining permission to conduct the study. In Vienna it was possible to contact the school directors directly with provided documents. Ultimately, the questionnaire was distributed to teachers in all federal states but Salzburg through their respective directorates.

#### 4.4 Survey

The survey was administered via an online questionnaire designed to be self-explanatory to teachers. An explanation was provided for each question to ensure the comprehensiveness of responses. To increase participation rates, the key arguments for conducting research in this area were presented before the survey. No incentives, such as gifts or other rewards, were offered to participants to discourage perfunctory or insincere responses.

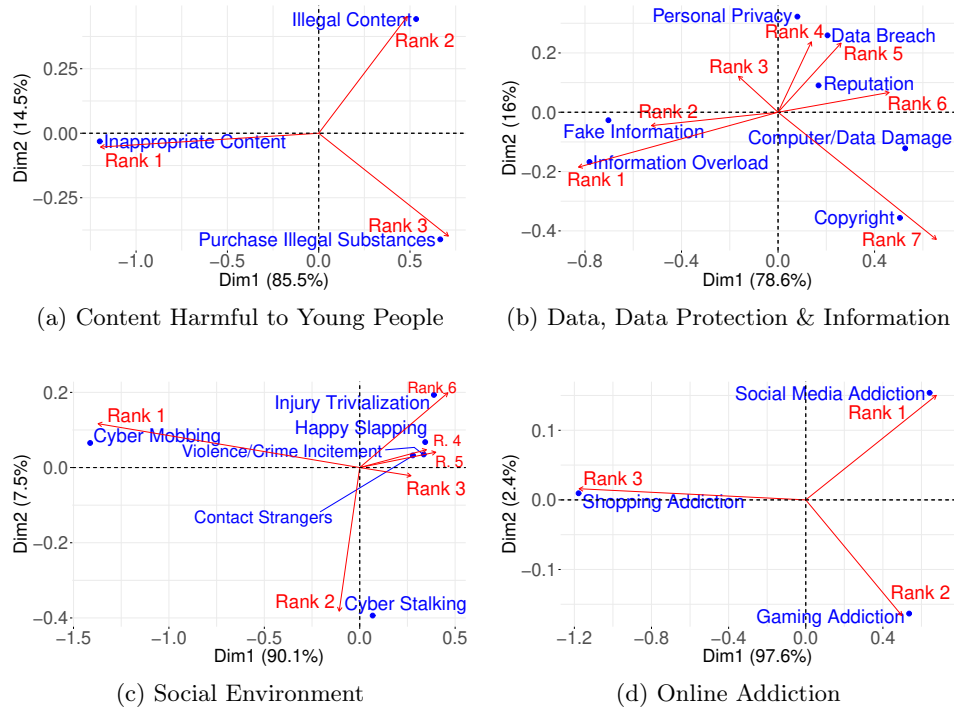
### 4.5 Findings

Note that the following representations and insights are based on data collected from the perspective of teachers. In figure 1a the box-whisker-plot shows that teachers overall rate the average age at which children and teenagers use the internet without restrictions at 9.04 years ( $\pm 2.44$  years). Taking a closer look at the data, it can be observed that female teachers estimate the age at which children use the internet without restrictions to be 8.89 years ( $\pm 2.28$  years), slightly lower than their male peers who estimate it to be 9.36 years ( $\pm 2.70$  years). When considering the data from the perspective of different generations, slight differences can be observed. Especially teachers belonging to the Baby Boomer generation report the highest age estimation at 9.60 years ( $\pm 2.49$  years), while those from Generation Z specify the lowest at 8.12 years ( $\pm 2.32$  years).



**Fig. 1.** Internet usage and teachers’ experience regarding digital threats

Figure 1b illustrates the proportion of teachers who have already experienced at least one case first-hand in relation to digital threats for children or teenagers as well as the proportion of teachers with indirect experience. The chart in figure 1b suggests that 71% of all teachers have personally witnessed or become aware of children or teenagers being involved in at least one of the mentioned digital threats. When considering teachers who also know someone who has witnessed such a case, the percentage increases to 90%. Observed from different perspectives, the following values emerge. For example, 72% of female and 70% of male teachers acknowledge having had first-hand experience, while 90% of female and 88% of male teachers state having had at least indirect experience. Considering the perspective of different generations [8], 65% of teachers belonging to the Baby Boomer generation, 69% of Generation X, and 77% of Generation Y state that they have already had first-hand experience. When including indirect experience, 85% of the Baby Boomer generation, 89% of Generation X, and 92% of Generation Y indicate having respective experience. From the view of federal states, corresponding values range from 61% to 79% with regards to first-hand experience and from 84% to 94% when including indirect experience as well.



**Fig. 2.** Ranking of threats within their respective categories

During the questionnaire, teachers were asked to rank the threats within the specified categories based on the frequency at which children and teenagers are exposed to them. The analysis yielded the following patterns by utilizing classical correspondence analysis (CA). When using CA, the correlation or association between a category (here: threat) and a specific rank is not solely based on the relative frequency of the category in that rank. CA considers the joint distribution of categories and ranks to calculate the associations. The association of a category with a specific rank is determined by various factors, including the shared variation in the data and the relative positioning of categories and ranks in the analysis. Figure 2 illustrates the relationship between threats and their respective ranks within each category. The variance of the data in the categories of “Content Harmful to Young People” as well as “Online Addiction” is completely determined by the first two dimensions, since there are only three threats. In particular, for the latter, the first dimension shows significant dominance. The variance of the data in the categories of “Social Environment” and “Data, Data Protection & Information” is determined by the first two dimensions to 97.6% and 94.6% respectively. These are described by a total of six and five dimensions.

#### 4.6 Validity

Regarding internal validity the following considerations have been taken into account. Teachers may tend to select their responses based on societal expectations, potentially overrating or underrating certain threats. In addition, negative experience with particular threats may influence teachers' ranking of those in contrast to such with no first-hand experience. Moreover, teachers may have difficulty remembering specific incidents or events. The distribution of teachers by gender corresponds to that of the total population, which has a positive impact on representativeness. Furthermore, the absence of the state of Salzburg is not expected to be a major source of error. Concerning external validity, it can be said that the selected schools were chosen randomly. The participating schools were asked to communicate their participation to all teachers. Since teachers participated voluntarily, there is a chance that teachers with an opinion or experience about the topic were more likely to participate in the survey than those with no prior experience in this area. The online questionnaire measurement instrument was designed to mitigate systematic errors or biases. For example, the starting position for rankings was randomized for each participant and active response was required for all questions without default values. Teachers could decide on their own when to participate. The setting did not pressure teachers to participate or promise a thank-you gift.

### 5 Discussion

As part of the questionnaire, teachers were asked to estimate at what age they think children and teenagers have unrestricted access to the Internet. The mean value of all responses suggests 9.04 years ( $\pm 2.44$  years). Figure 1a shows that 50% of responses are between 7 and 10 years. Furthermore, the median and mean equal 9 which indicates a symmetric distribution of the data with few outliers, reducing its bias. Considering different perspectives such as gender, generations or federal states, the mean value only varies slightly. The determined value suggests that children already have unrestricted access to the Internet during primary school. On the one hand, this can contribute to early learning of digital technologies; on the other hand, it makes them more vulnerable to facing digital threats at an early age. Additionally, as shown in figure 1b, 71% of teachers report having personally experienced or witnessed an incident related to digital security threats. Another 19% state knowing someone who has experienced or witnessed such a case. Combined, 90% of all participating teachers have either encountered at least one case themselves or know someone who has. Another result of this study has been published at the ISSEP 2023 conference [15], which illustrates teachers' experience and awareness of digital threats to children and teenagers. Comparing the ranking of these threats based on teachers' first-hand experience with their own ranking reveals a consistent pattern. Instead of using relative frequencies, the ranking of threats was based on the use of CA. The idea behind this approach is to better understand the association of threats with ranks. The goal is not to identify the absolute highest-ranked threat but to get a sense of

what teachers have already experienced and how threats are ranked within their respective categories. By using CA threats are not only assigned to fixed ranks, instead, an association with various ranks can be observed. While performing the CA, multiple dimensions are identified that describe different characteristics of the data. Depending on the data, our analyses yield two to six dimensions. It is important to note that the interpretation of the diagrams only considers the first two dimensions, which capture the majority of the variance of the data. Doing so allows a small margin of interpretation error, but in our case, it can be neglected. Figure 2a suggests that in terms of threats in the category of “Content Harmful to Young People”, the threat *Inappropriate Content* is strongly associated with rank one, and teachers reported to have the most experience with incidents of this. The same applies to second-ranked *Illegal Content* and third-ranked *Purchase Illegal Substances*. Furthermore, in illustration 2b, the ranking of threats in the category of “Data, Data Protection & Information” unveils that some ranks have minimal influence on the data structure. The threat *Information Overload* is most strongly associated with the first rank, followed by *Fake Information*, showing a visible connection to the first rank. Rank three does not show a strong association with any particular threat. This could be due to one or more threats being frequently ranked at rank three while being equally ranked at other ranks as well. It may indicate that the rank is not relevant. Following threats are associated with multiple ranks. Rank four shows the strongest association with *Personal Privacy* and *Data Breach*, with the latter also associated with the fifth rank. *Reputation* lies between the fifth and sixth rank. *Computer/Data Damage* is associated with ranks six and seven, with *Copyright* strongly associated with rank seven, although there is some influence from rank six. In this category, ranks one and seven have the most significant influence on the data structure, followed by rank two and six. Comparing ranking with the teachers’ personal experience regarding threats shows a strong similarity of the ranking and frequency of experience with *Information Overload* and *Fake Information*. The same can be observed for many threats. Examining figure 2c shows that in the category “Social Environment” *Cyber Mobbing* stands out by being ranked significantly higher than other threats at the first rank. The threat *Cyber Stalking* can be strongly associated with rank two. No threat in this category indicates a strong association with rank three. Ranks four and five are very close to each other. *Violence/Crime Incitement* and *Contact Strangers* both have a strong association with rank four and five with a slight inclination towards rank three as well as *Happy Slapping* with a slight inclination towards rank six. Furthermore, *Injury Trivialization* is strongly associated with the sixth rank, although there is also an influence from other ranks. Comparing these findings with the teachers’ personal experience, both show a noticeable leap from *Cyber Mobbing* to *Cyber Stalking*, followed by a distinct transition to the other threats. Finally, as shown in figure 2d, the category “Online Addiction” is straightforward to interpret. The first ranked *Social Media Addiction* and second ranked threat *Gaming Addiction* are mutually associated, while *Shopping Addiction* associated with rank three

is independent and points in the opposite direction. This pattern is consistent with teachers' personal experience.

## 6 Conclusion

Most publications prioritize competencies for digital media, neglecting competencies required to handle digital threats. Existing publications provide limited lists of threats each and emphasize impacts. This paper categorizes known threats of various publications into four categories and ranks them based on teachers' assessments. Findings reveal alignment between teachers' experience and rankings, highlighting numerous digital threats children and teenagers face. The findings suggest that children and teenagers are exposed to digital technologies such as the Internet at an early age. Teachers realize that young people are confronted with threats in this area. At the same time, they are the ones who will play a vital role in the future in teaching the necessary competencies in this regard. Regarding curricula, there are significant regional differences. In Austria, for example, curricula are centrally determined for all federal states. In Switzerland, federal guidelines are provided, but the cantons translate these into their curricula. A similar system exists in Germany. There are numerous curricula with often loosely defined requirements regarding competencies in digital security. All those differences and available formulations make assessing which competencies are being taught to address such threats challenging. Although the teachers' point of view provides a unique insight into what threats in the field of digital security are relevant to children and teenagers, this should not be taken as the sole truth. For this reason, further surveys of pupils and parents will be carried out. In the course of a dissertation, exploring this issue will involve investigating the relevant threats faced by children and teenagers at different ages. Additionally, the focus will be on gathering, defining, and structuring the competencies required to address these identified threats effectively.

## References

1. Bundesministerium für Bildung, Wissenschaft und Forschung: Gesamte Rechtsvorschrift für Lehrpläne der Volksschule und der Sonderschulen. StF: BGBl. Nr. 134/1963 idF BGBl. Nr. 267/1963 (DFB). Änderung BGBl. II Nr. 1/2023
2. Bundesministerium für Bildung, Wissenschaft und Forschung: Gesamte Rechtsvorschrift für Lehrpläne – allgemeinbildende höhere Schulen. StF: BGBl. Nr. 88/1985. Änderung BGBl. II Nr. 1/2023
3. Bundesministerium für Bildung, Wissenschaft und Forschung: Schulen-Online (2023), <https://www.schulen-online.at>
4. Bundesministerium für Inneres, Bundeskriminalamt: Polizeiliche Kriminalstatistik 2022: Die Entwicklung der Kriminalität in Österreich (2023), [https://bundeskriminalamt.at/501/files/2023/PKS\\_Broschuere\\_2022.pdf](https://bundeskriminalamt.at/501/files/2023/PKS_Broschuere_2022.pdf)
5. D-EDK: Lehrplan 21. Gesamtausgabe. Bereinigte Fassung. Deutschschweizer Erziehungsdirektoren-Konferenz, Luzern, Switzerland (2016), [https://vfe.lehrplan.ch/container/V\\_FE\\_DE\\_Gesamtausgabe.pdf](https://vfe.lehrplan.ch/container/V_FE_DE_Gesamtausgabe.pdf)

6. Eichenberg, C., Auersperg, F.: Chancen und Risiken digitaler Medien für Kinder und Jugendliche: ein Ratgeber für Eltern und Pädagogen. Hogrefe, Göttingen, Germany, 1 edn. (2018)
7. Gasser, U., Cortesi, S., Gerlach, J.: Kinder und Jugendliche im Internet: Risiken und Interventionsmöglichkeiten. hep, Bern, Switzerland, 1 edn. (2012)
8. Klein, C.: Jede Generation hat eigene Werte – Generation Z. *physiopraxis* **18**(1), 58–60 (2020). <https://doi.org/10.1055/a-0975-1796>
9. Külling, C., Waller, G., Suter, L., Willemse, I., Bernath, J., Skirgaila, P., Streule, P., Süss, D.: JAMES - Jugend, Aktivitäten, Medien - Erhebung Schweiz. Zürcher Hochschule für Angewandte Wissenschaften, Zurich, Switzerland (2022)
10. Medienanstalt Rheinland-Pfalz: [klicksafe.de](https://www.klicksafe.de/en): The EU initiative for more safety on the net (2023), <https://www.klicksafe.de/en>
11. O’Keeffe, G.S., Clarke-Pearson, K., on Communications, C., Media: The Impact of Social Media on Children, Adolescents, and Families. *Pediatrics* **127**(4), 800–804 (Apr 2011). <https://doi.org/10.1542/peds.2011-0054>
12. Reid Chassiakos, Y.L., Radesky, J., Christakis, D., Moreno, M.A., Cross, C., COMMUNICATIONS, C.O., MEDIA, Hill, D., Ameenuddin, N., Hutchinson, J., Levine, A., Boyd, R., Mendelson, R., Swanson, W.S.: Children and Adolescents and Digital Media. *Pediatrics* **138**(5) (Nov 2016). <https://doi.org/10.1542/peds.2016-2593>, e20162593
13. Senatsverwaltung für Bildung, Jugend und Familie: Rahmenlehrplan 1-10 kompakt: Themen und Inhalte des Berliner Unterrichts im Überblick. Senatsverwaltung für Bildung, Jugend und Familie, Berlin, Germany, 1 edn. (2017), [https://www.berlin.de/sen/bildung/unterricht/faecher-rahmenlehrplaene/rahmenlehrplaene/rlp\\_kompakt\\_1-10.pdf](https://www.berlin.de/sen/bildung/unterricht/faecher-rahmenlehrplaene/rahmenlehrplaene/rlp_kompakt_1-10.pdf)
14. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., Hasebrink, U.: EU Kids Online 2020: Survey results from 19 countries. *EU Kids Online* (2020). <https://doi.org/10.21953/lse.47fdeqj01ofo>
15. Taupe, J., Knapp, V., Bollin, A.: Teachers’ Experience Regarding Digital Threats for Children and Teenagers. In: 16th International Conference on Informatics in Schools, ISSEP 2023, Local Proceedings. Zenodo, Lausanne, Switzerland (Oct 2023). <https://doi.org/10.5281/zenodo.8432020>
16. Tintori, A., Ciancimino, G., Bombelli, I., De Rocchi, D., Cerbara, L.: Children’s Online Safety: Predictive Factors of Cyberbullying and Online Grooming Involvement. *Societies* **13**(2) (2023). <https://doi.org/10.3390/soc13020047>, <https://www.mdpi.com/2075-4698/13/2/47>