THE STATE OF KNOWLEDGE OF TEACHERS AND EDUCATORS IN PRIMARY AND SECONDARY EDUCATION ON CYBER THREATS CHALLENGING STUDENTS ON A DAILY BASIS - PROPOSAL OF PREVENTION AND TRAINING AREAS

D. Siemieniecka, K. Majewska

The Nicolaus Copernicus University in Toruń (POLAND)

Abstract

Cyber threats are a huge problem and a challenge for educators working in schools. As statistics show, the probability of a specific threat varies with the age of the students. Younger children (owing to the lack of mental and emotional maturity and awareness of threats) are more exposed to extortion, fraud, cyber-pedophile attacks, misunderstanding of online messages, theft of personal data, or contact with messages that are not adapted to their age. Older children - by establishing contacts with people they do not know, they may become victims of such crimes as: extortion of funds, cybersex, pornography, and prostitution, they may also be harassed or become victims of stalkers. These threats may be transferred to the real life of a young person, resulting in depression and, in extreme cases, suicide attempts. When establishing their first emotional and intimate relationships young people share their personal photos that can be published or become the cause of blackmail. By participating in social life, they comment, praise, but also ridicule, offend, and hurt the feelings of others. They are inspired by fashion and behaviour promoted on line. Taking up online challenges, e.g. on TikTok, can result in bodily harm, disability, and even loss of life. These threats and their physical and mental consequences may be long-term and determine young people's further lives and choices. In order to prevent the above-mentioned phenomena, preventive measures should be implemented in order to familiarize students with the risks and ways of counteracting them. These measures should be undertaken as early as possible by educating family and teachers.

The text of the article will present the results of a pilot study showing the state of teachers' knowledge about cyber threats to which students are exposed. The research was carried out in 2021-2022 and covered a group of 250 primary and secondary school teachers. On the basis of the research, the authors prepared a report summarizing the state of teachers' knowledge about the risks to which students are exposed in the Internet space. The text will define the areas related to the training needs connected with the undertaken topic.

Keywords: in-service teacher training, teachers knowledge, school, education, cyber threats.

1 INTRODUCTION

From birth, children grow up in a world of which new technologies, the Internet, and mobile devices are an integral part. Interesting research on the use of mobile devices by children aged 0-6 was carried out in July 2020 by Magdalena Rowicka and Michał Bujalski. The report from the research drafted by them was entitled: "A Tot on the Net - the Phenomenon of Using Mobile Devices by Children Aged 0-6". The quantitative research covered 2,000 parents (with children aged 0-6), while the qualitative research covered 48 parents and 60 children [1]. The research results which were included in the report indicate that 54% of children aged 0-6 use smartphones, tablets, smartwatches, and laptops. The authors write that "the average age of initiation into using mobile devices is 2 years and 2 months of age. Most children use mobile devices that have access to the Internet (they are online) (75%). Children aged 0 to 6 use mobile devices for more than 1 hour a day on average. Most children use only content aimed at children (movies, cartoons, games, colouring books, etc.) (88%). Almost three out of four children aged 0 to 6 use mobile devices when traveling by car (or other means of transport), every second child during meals, and every ninth child while using the toilet" [1].

Recent reports from the research indicate that 40% of children aged 8-12 get connected to the Internet every day. Among teenagers (children 13-16 years old), regular Internet users account for as much as 89% [2].

One of the most important reports published in Poland on the use of the Internet by young people was prepared by a team led by Maciej Tanaś. It was published by NASK National Research Institute in 2016 under the title "Teenagers 3.0. Selected results of the nationwide study of students in schools " [3]. The content of the report describes the activity of young people in the Internet space, who experience in relations with other Internet users: insults (32% N = 442), humiliation, ridiculing (19.4%, N = 265), frightening (13.6%, N = 186), impersonating another person (12.6%, N = 172), spreading compromising messages (12.4%, N = 169), and blackmailing (11.1%, N = 151). Young people also observe the phenomena of violence directed towards their colleagues; this includes “calling their friends names (59.7%) as well as humiliating and ridiculing them (58.1%). Disseminating compromising materials about their friends was declared by 33.3% of the respondents. Frightening friends was indicated by 34.2%, while blackmailing them via the Internet by as much as 24.4%” [3]. The results of this research show how important it is to educate young people in the area of acquiring competences in the field of safe use of the Internet, communication skills, sharing information about oneself, and responding appropriately to forms of psychological violence (expressed verbally). Other surveys were carried out as part of the social campaign "Violence on the Internet leaves invisible wounds", and the project "Youth 13+ supported and under the care of the Association 'SOS Children's Villages in Poland' " (these surveys were conducted in 2020 and 2021) show the frequency of using the Internet by young people who declare that they use it all the time (30% of the respondents, N = 238), while 59% that they use it several times a day. The authors of this study touched upon a very important issue, namely the emotions felt by young people, related to the experiencing of various forms of cyberbullying (e.g. behaviours such as humiliation, frightening, blackmailing, verbal abuse, impersonating, and disseminating degrading materials) [4]. 34.7% of the young people surveyed did not inform anyone about the experienced cyberbullying, 24% of the young people confided in a friend/colleague, 12% shared their problem with their parents. Unfortunately, only 3% of the respondents reported the matter to the school educator, and 1.3% to their teacher. Young people react to violence with indifference (21% of the respondents), sadness (15%), anger (14%), and fear (11%). 38% of the respondents declare that they have not experienced any cyberbullying [4]. A survey carried out on a group of 737 students by the Supreme Audit Office shows that "half of the surveyed students (...) in the case of experiencing cyberbullying would not turn to anyone for help, while just over 13% of the students would turn to a teacher for help, and 19% to their parents" [5]. The same report states that “cyberbullying is a serious problem among students. Almost 40% of the students, almost 30% of their parents, and 45% of the surveyed teachers” encountered this phenomenon [5].

In 2020, the report "EU Kids Online 2020" [6] was published. The research results contained in it concerned the application of a comparative approach to the use of the Internet by children from 19 European countries [7]. In Poland, this project was carried out by a research team consisting of Jacek Pyżalski, Aldona Zdrodowska, Łukasz Tomczyk, and Katarzyna Abramczuk. Polish children use the Internet via mobile devices such as a mobile phone and a smartphone. 84% of the surveyed children use the Internet every day. Half of 9-10-year-olds have their own profiles on social networks. Young people mainly use the Internet for entertainment and to communicate with others (friends, family members). The Internet is also an important tool used, especially by young people, for learning and engaging in social activities. Some conclusions from the research are consistent with the currently published reports. The Office of Electronic Communications has published two reports on nationwide research on Internet use, carried out in 2021 [8]. One of them covered children and their parents, while the other covered teachers. A total of 500 children and their parents were included in the study. The group included children aged 7-9 (36% of the study group), 10-12 years of age (41% of the study group), and 13-14 years of age (23% of the study group). The children’s statements were compared with the parents’ opinions in the distinguished categories, which made it possible to check the parents’ knowledge about the use of the Internet by their children. The results of the analyses show that 79% of children have a mobile phone. Children start using it at the age of 7-8 (46% of the surveyed children). 57.8% of the surveyed group of parents notice the negative impact of mobile phones and the Internet on the development of children (which was indicated by 66.7% of the surveyed parents). Children use the Internet every day, spending 2 hours there (in addition to Internet during school education). Parents try to control their children’s activity on the Internet and take care of their safety by setting the rules for using it together with them (73% of the children, 67% of the parents), using special applications (32% of the children, 42% of the parents), setting up safety functions in a mobile phone (29% of the children, 38% of the parents), and the use of safe starters for the youngest children (14% of the children, 16% of the parents) [8]. In the 2018 report from the opinion poll carried out by the Public Opinion Research Centre (CBOS), we find the information that 86% of the parents limit the time that 6-12-year-olds spend on the Internet, while 75% of the parents limit it to 13-15-year-olds [9]. Children using the Internet watch YouTube videos (73%), play games (69%), communicate with family and friends (55%), browse websites (48%), listen to music (45%), and use social media websites (43%) [8]. Research [8] on the threats to which children were exposed in the Internet space (and which their parents witnessed) and the protection of privacy used by children is particularly interesting in the context of the discussed issues. 38% of the children publish content on social media websites. Among the children using social networking sites, 60% do not provide their password or login to portals, 60% of them do not send pictures to strangers, 32% use passwords that are difficult to decipher, 31% of the posts posted by the children have set restrictions on access to the group of their friends. 12% of the children do not use any method of securing access to information about themselves that is private. The parents say that 41% of the children know how to make purchases on the Internet, but 76% of them indicate that the children do not do it on their own. The report deals [8] with the negative phenomena which children using the Internet are exposed to. 60% of the children have not experienced the risk situations mentioned by the researchers in the survey. 17% of the children have come across images or videos presenting violence on the Internet (43% of the surveyed children indicated this phenomenon as frequent), 14% have found drastic content presenting diseases or bodily injuries (images, films) (33% of the surveyed children considered this phenomenon as frequent), 14% have seen hate and hate speech (50.8% indicated this phenomenon as frequent), 11% have encountered nudity and sexual acts (46% of the children indicated this phenomenon as frequent), 9% of the children have met strangers via the Internet, 7% have encountered vulgar comments about them on the Internet, 6% of the children have experienced exclusion by their friends, 5% have been oppressed by posts on social networks. 4% have experienced the effects of access to their photos, videos by an inappropriate person, 3% of the surveyed children have experienced a situation in which another person has posted a video or content ridiculing them [8]. The parents of the children are primarily concerned about the fact that children will establish dangerous contacts via the Internet (58%, N = 173) with paedophiles, perverts (30%, N = 173), will come across inappropriate content (33%), pornography (17 %), violence, violent, brutal scenes, aggression in movies and games, vulgar language (5%), threats related to information and financial security (18%), disclosure of personal data (7%), harassment, hate (6%), Internet addiction (6%), contact with sects (2%), access to drugs, legal highs, alcohol (6%), and false information (1%) [9]. The studies cited here lack analyses of the new phenomena described in the Cybersurvey Report. These studies were conducted by Adrienne Katz and Aiman El Asam as part of Youthworks in collaboration with Internet Matters.org [10]. The results of the research showed that the number of children (currently, it is 28%) who view harmful content related to the change of their body (e.g. building the body through supplementation with products that are dangerous to health) is increasing, 23% view content related to anorexia, 25% of the children have had contact with suicide-related content. 26% of the respondents have had contact with images of violence that they did not want to see, 23% have watched nudity, 20% of the children have been offered illegal goods, 19% have been induced to undertake risky behaviours (challenges), 20% have watched materials encouraging violence [11].

It can be seen that teachers, guardians, and parents of children face new problems that require prophylaxis and prevention of pathologies. Only educational activities have a chance to balance this negative influence of the Internet on the body and spiritual development of a young person.

1.1 Categories of cyber threats

In the literature of the subject [12, 13], the following types of cyber threats are distinguished:

- Cyber harassment - this is harassment involving the sending of aggressive, ridiculing messages by the sender (e.g. Via instant messaging). These messages can be intimidating, hurtful, judgmental, or blackmailing the victim.
- Flaming - this is a public exchange of views on a forum, which is characterized by aggression.
- Identity theft (impersonation) - is the impersonation of another person, creating an account by the perpetrator under the victim's name and surname or using the victim's login details (e-mail, social networks) known to the perpetrator.
- Making secrets public (outing) - dissemination by the perpetrator of private materials related to the victim, e.g. Photos, films, correspondence.
- Cyberstalking - tracking activity and harassing the victim via online tools [24].
- Happy slapping - an aggressive physical attack on a random person, recorded digitally in the form of a video or photo and shared on the internet.
- Denigration - sharing by the perpetrator of humiliating and degrading materials (photos, videos, information) about the victim.
- Exclusion - consists in removing from the contact list, deliberately omitting such a person in the group.
- Technical aggression - includes the destruction of equipment through deliberate actions consisting in sending viruses, trojans, hacking into computers using e-mail or social networking sites.

1.2 Actions taken by the Ministry of Education

On the website of the Supreme Audit Office (SAO), we learn about the results of inspections in the field of preparation for counteracting the phenomenon of cyberbullying among children and adolescents [14].

The inspection covered state bodies and institutions, such as The Ministry of National Education, Ministry of Digital Affairs, schools, and the Police. On the website of the Supreme Audit Office, we read that these authorities “did not properly recognize or define the scale of the threat posed by cyberbullying among children and adolescents. The Ministry of National Education did not coordinate activities in the field of preventing and counteracting cyberbullying among students, nor has it developed any guidelines on cyberbullying, e.g. for schools. As a result, each of the inspected schools developed appropriate rules of conduct independently, on their own. The Police, in turn, carried out preventive measures in schools, provided that principals reported such a demand. It is, therefore, not surprising that most incidents of cyberbullying are not disclosed, although students and teachers admit in the surveys that cyberbullying affects more than 1/3 of students. On the other hand, SAO positively assesses the actions of schools in response to reported acts of cyberbullying" [5].

In 2017, the Ministry of National Education developed a set of recommendations and guidelines addressed to school principals and governing bodies, entitled “Safe School. Response procedures in the event of internal and external physical threats in the school" [15]. Other documents developed as part of Safe School concerned preventive measures [16] and a compendium of knowledge prepared especially for school principals [17]. On the basis of this package of recommendations, schools developed internal procedures for responding to threats related to, among others, cybersecurity [18].

2 METHODOLOGY

The research presented in the text was carried out in 2021 and 2022, in a group of 251 teachers of schools of various levels, working throughout the country. The selection of the research group was random. The actions taken were based on the diagnostic survey method (a questionnaire, partially directed interview) supported by statistical methods (knowledge test). The conclusions were mainly based on quantitative data supplemented with a qualitative analysis. The main goal of the presented project was to test teachers’ knowledge of cyber threats occurring in school, as well as to verify their ability to deal with them. The research analysed the relationship between age and the subject taught and teachers’ knowledge of cyber threats and ways of dealing with them; the fact of being a class teacher and the level of awareness of threats; the type of school in which teachers work and the level of awareness of threats. As a result, the following research objectives were identified:

1 Determining the level of teachers’ knowledge about cyber threats occurring in school, ways of preventing and addressing them;

2 Determining the educational needs of teachers in the field of cyber threats.

Among the identified specific problems, the following were formulated:

1 Are teachers familiar with issues related to cyber threats?

2 How do teachers rate their level of knowledge of cyber threats?

3 Where do teachers find out about cyber threats?

4 In the event of a cyber threat in school, would teachers be able to help the student?

5 Do teachers take any steps to prevent cyber threats as part of their educational activities?

6 Do teachers feel the need for any additional training and are they getting trained about cyber threats, ways of preventing and addressing them?

7 What would teachers expect from courses dealing with cyber threats?

Statistical significance was verified using Chi square tests as well as appropriately determined correlations.

3 RESULTS

The conducted research has shown that the vast majority of teachers are aware of the seriousness of the problems resulting from cyber threats. 94.8% of the respondents answered that the teacher should be aware of the dangers that their students face on the Internet. The above response gives hope for an improvement in the situation, because the knowledge teachers have is much smaller than that declared by them in their individual self-assessment.

The responses show that teachers assess their knowledge of cyber threats as:

- Very good - 31.9%,
- Good – 47.8%,
- Satisfactory - 17.1%.

3.2% of the respondents rated their knowledge lower than satisfactory. In fact, every fifth teacher is not able to give specific examples of threats related to students and the space of the Internet, using the general term ‘cyber threat’. 11.16% of the respondents mentioned only one known threat when commenting on cyber threats. 53.38% mentioned two examples of threats, and 15.14% mentioned three or more. One of the respondents replied that she did not know any threats lying in wait for students in the Internet space (0.4%).

Teachers confuse terminology related to cyber threats. They do not know the division of cyber threats into specific types. The knowledge test developed for the purposes of the research showed that:

- 96.41% of educators cannot properly explain the definition of sexting, mistaking it for sex on the Internet or viewing pornography.
- 56.57% cannot properly describe what cyberbullying is,
- 64.54% do not know what flaming is,
- 90.44% have never heard the phrase ‘child grooming’,
- 45.42% of teachers think phishing is searching for potential victims on the Internet.

Certainly, teachers are aware that young people send intimate photos or post them on social networks, but they cannot name the phenomenon correctly. Educators know about arguments and online harassment, but are not aware of the scale of the phenomenon. Everyone is scared of online paedophilia, but they do not associate it with child grooming, etc. Most of the teachers surveyed are not aware of all the risks that their students may face. Less than 3% of the respondents have heard about dangerous challenges, and only one person used the term "blue whale" in the survey (“Blue *whale*” is an online game consisting in taking up challenges issued by a virtual "guardian". They are to deal with, for example, mutilating one’s own body). Therefore, the knowledge of educators in the field of cyber threats is general, incomplete, and needs to be supplemented. The same is true in the context of their knowledge of preventing or helping victims of Internet violence. As a consequence, many teachers would not be able to properly guide and help victims of cyberbullying. This problem affects all age groups as well as people working in primary and secondary schools. However, in the course of the research analysis, it was noted that people over 56 years of age showed a lower level of knowledge in this area than their younger colleagues. A comparison of teachers representing various subjects shows that the knowledge of IT specialists seems to be a bit broader, but also needs to be supplemented. This is all due to the fact of dynamic changes and constantly emerging new threats that seem to be alien to educators.

Among the online threats they are familiar with, teachers mention: hate (41.43%), bullying (7.97%), identity theft (11.16%), data theft (1.99%), phishing (1.99%), sexting (3.98%), paedophiles (9.16%)), pornography (6.77%), stalking (0.8%), dangerous challenges (2.79%), computer games (18.73%), scenes of violence (11.95%), content not adapted to age (21.51%), gambling (1.59%), free access to any topic (7.71%), viruses (4.78%), malware (3.98%), micropayments (0.4%), publishing vulgar photos (1.99%), contacts with people providing false information (4.78%). 19.92% of the respondents answered that cyber threats are the threats children face online.

The risks occurring in school noticed by teachers include:

- Hate (53.39%)
- Access to inappropriate content (8.37%),
- Students sending each other e-mails with pornographic pictures (e.g. From the toilet), images showing mutilation, violence, etc. (9.56%),
- Vulgarisms on the web (2.39%),
- Ridiculing (6.77%),
- Harassment (4.78%)

- Addiction to the internet, games, social networks and applications (11.55%),
- Breaking passwords, using someone else's account (1.59%),
- Plagiarism, fraud (3.19%),
- Viruses (1.2%),
- E-mails with viruses (0.8%),
- Pornography (12.35%),
- Sexting (0.4%),
- The accosting of female students by much older men (0.4%),
- Paraphilias (e.g., persuading to send shoes, clothes) (0.4%),
- Stalking (0.8%),
- Computer hacking (1.99%),
- Grooming (0.8%),
- Phishing (1.99%),
- Flaming (0.4%),
- Trolling (0.4%).

3.98% of the respondents did not notice any cyber threats in the school they work for. One of the teachers even noted that "Children in my school do not use smartphones and the Internet, so the problem of cyber threats does not concern our facility".

As demonstrated by the research, the sense of responsibility for students' cybersecurity declared by teachers is ambiguous. On the one hand, teachers answer that each teacher (regardless of the subject taught) should prepare students to use the Internet safely, whenever possible (72.5% of the respondents), on the other hand, they emphasize that this obligation should lie mainly with IT teachers (23.5%), class teachers (39.4%), and school counsellors (30.7%). In addition, teachers associate the cybersecurity of children with the activities of services such as the police or municipal police (28.7%), and with the educational role of the family (51%).

The Safer Internet Day has been celebrated in the calendar of Polish schools for several years (in some schools it is even the Safer Internet Week). As part of them, celebrations, art competitions, knowledge competitions, as well as lessons aimed at preventing the safe use of the Internet are organized. The analysis of the collected data shows unequivocally that IT teachers and class teachers are primarily involved in preventive measures in this regard. They download educational materials for lessons from the websites of NASK and the Empowering Children Foundation. Some of them use computer science textbooks. The answer to the question: do you think communicating knowledge about safe online behaviour is a difficult task? divided teachers into almost numerically similar groups. The former believes that talking about cyber threats is a difficult task (44.6%) while the latter that it does not cause them much trouble (55.4%).

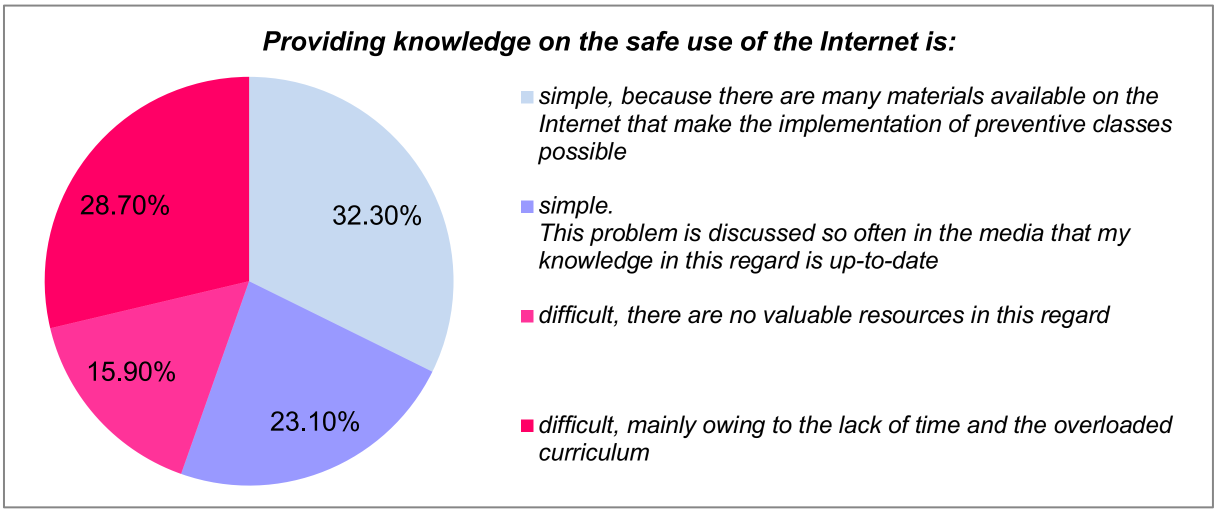

Chart 1. *Teachers' opinions about providing information on online safety.*
Source: *Own study*

The provided answers show that teachers find out about cyber threats and ways of preventing them mainly on their own from the Internet, which is declared by 64.1% of the respondents. Slightly fewer of them - 58.2%, find out about Internet threats on their own from television, books, or newspapers. 54.6% supplement their knowledge about cyber threats through various types of courses. 9.6% of teachers declare that they found out about the threats of cyberspace during their studies in junior high school, senior high school, and at college/university.

Most teachers declare that they would like to find out more about cyber threats and ways of preventing and addressing them. 60.96% of the respondents indicated that they would prefer to take part in on-line training, while 39.04% - in offline courses.

4 CONCLUSIONS

The studies available in the Polish literature indicate that the most common problem of students is the communicative forms of network violence, such as insults, hate, ridiculing, harassment, etc. The analyses carried out and presented in the text show that some teachers also see other serious threats and problems occurring among students such as, for example, sexting, various types of paraphilias, pornography, and paedophilia. In addition to problems of a sexual nature, in schools one can also encounter phishing, flaming, trolling, hacking, stalking, plagiarism, network addiction, etc.

Based on the research carried out by the authors of this text, it can be concluded that teachers' knowledge of cyber threats is superficial, unregulated, unstructured and, above all, out of date. Teachers as well as class teachers know that there may be problems with the use of technology among students, but the vast majority of them are not able to name them correctly, describe them and, most importantly, indicate options for solving a problem and forms of helping victims of violence. Worryingly, teachers and educators are not among the people to whom students report the problem of cyberbullying. Therefore, the content in the curricula should take into account the ways in which students deal with difficult situations such as being a victim or witness of cyberbullying. It is, therefore, necessary to build an integrated school and educational environment based on the trust and integration of class and school communities.

It is also important to take steps to develop an educational and psychological training cycle that would help to supplement the knowledge of educators, as well as understand the problems encountered by students. In addition to subject competences, teachers should have knowledge about the risks accompanying young people, as well as the consequences of their occurrence (such as, for example, withdrawal, lowered self-esteem, fear, phobias, and even depression).

Safety training for teachers should be carried out on a regular basis and cover different levels of knowledge and skills depending on the previous diagnosis [25]. Training content should certainly comprise [19]: 1. legal aspects related to cyberbullying, 2. preparation of teachers to recognize changes in students' behaviours that attest to the experiencing of the phenomenon of cyberbullying (e.g. bullying, seduction), 3. preparation to recognize and counteract the phenomenon of Internet addiction, as well as cooperation with parents in in this regard, 4. discussion of the forms of assistance offered by institutions implementing the therapy, 5. showing the principles of online communication and image protection, proper interpersonal communication, and forms of reacting to the phenomena of verbal violence, 6. presentations of creative and developmental aspects of the Internet and alternative forms of spending time 7. information making possible the development of students' self-esteem and acceptance of their own body, 8. materials promoting the development of empathy and morality, 9. data on the security of the IT infrastructure of the school and class, 10. presentation of techniques and methods of group work and building a community based on transparency, respect for dignity, and subjectivity [19]. Certainly, the scope of this content is only indicative. Detailed issues would need to be specified.

The content and skills provided should support the resources intended for work with children and adolescents [20], because, as research shows, in the context of working with new technologies [21] Polish teachers are mostly a group of consumers, rather than creators [22].

It is worth emphasizing that some of the educational materials for teachers could be presented on-line, so reducing the implementation costs and facilitating access to the courses. Owing to the constantly developing level of computer technology, it is also worth recommending the implementation of training in virtual space, which ensures the high effectiveness of education [23].

REFERENCES

[1] M. Rowicka, M. Bujalski, "Brzdąc w sieci – zjawisko korzystania z urządzeń mobilnych przez dzieci w wieku 0-6 lat" (A Tot on the Net - the Phenomenon of Using Mobile Devices by Children Aged 0-6), https://www.kbpn.gov.pl/portal?id=15&res_id=11479398, Warszawa: Akademia Pedagogiki Specjalnej im. Marii Grzegorzewskiej, 2021.

[2] Micro Trend, "Report on the Internet safety of children 8-16 years old”, A survey conducted by 3D Market, commissioned by Trend Micro Polska in June 2020, https://resources.trendmicro.com/rs/945-CXD-062/images/RAPORT_trend%20micro_PL.pdf, 2020.

[3] M. Tanaś, W. Kamieniecki, M. Bochenek, A. Wrońska, R. Lange, M. Fila, B. Loba, "Teenagers 3.0. Selected results of the nationwide survey of students in schools", https://akademia.nask.pl/badania/RAPORT%20-%20Nastolatki%203.0%20-%20wybrane%20wyniki%20bada%C5%84%20og%C3%B3lnopolskich.pdf, Warszawa: NASK State Research Institute, 2016.

[4] SOS Children's Villages, "Youth 13+ supported and under the care of the Association ‘SOS Children's Villages in Poland’. The survey conducted as part of the social campaign „Violence on the Internet leaves invisible wounds”.", https://api.ngo.pl/media/get/150113, Warszawa, 2020.

[5] Supreme Audit Office, "NIK about cyberbullying among children and youth", https://www.nik.gov.pl/aktualnosci/nik-o-cyberprzemocy-wsrod-dzieci-i-mlodziezy.html, 2017.

[6] D. Smahel, H. Machackova, G. Mascheroni, L. Dedkova, E. Staksrud, K. Ólafsson, S. Livingstone, U. Hasebrink, "EU Kids Online 2020: Survey results from 19 countries. EU Kids, U Kids Online", London: The London School of Economics and Political Science, 2020.

[7] D. Siemieniecka, M.Skibińska, K. Majewska, *Cyberagresja: zjawisko, skutki, zapobieganie (Cyberaggression: the phenomenon, effects, prevention)*, Toruń: Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, 2020.

[8] UKE, "An opinion poll regarding the functioning of the telecommunications services market and preferences of consumers. Report on the children and parents survey", https://www.uke.gov.pl/akt/badanie-konsumenckie-2021-dzieci-rodzice-oraz-nauczyciele,412.html, 2021.

[9] CBOS, "A communication from the research of the Public Opinion Research Centre, Children and adolescents on the Internet - use and threats from the perspective of guardians", https://www.cbos.pl/SPISKOM.POL/2018/K_129_18.PDF, 2018.

[10] Internetmatters, "A new Cybersurvey report shows that a third of boys see online content that encourages them to gain mass", https://www.internetmatters.org/pl/hub/news-blogs/new-cybersurvey-report-shows-a-third-of-boys-are-seeing-content-online-encouraging-them-to-bulk-up/, 2020.

[11] A. Katz, A. El Asam, "In their own words The Digital Lives of Schoolchildren", https://www.internetmatters.org/wp-content/uploads/2020/10/Internet-Matters-CyberSurvey19-Digital-Life-Web.pdf, 2019.

[12] M.Skibińska, W.Kwiatkowska, K.Majewska, *Aktywność uczących się w przestrzeni Internetu (The activity of learners in the Internet space)*, Toruń: Wydawnictwo Naukowe UMK, 2014.

[13] J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży (Electronic Aggression and Cyberbullying as New Risky Behaviours of Young People),* Kraków: Oficyna Wydawnicza "Impuls", 2012.

[14] NIK, "Prevention and counteracting cyber violence among children and youth", https://www.nik.gov.pl/plik/id,15249,vp,17730.pdf, Warszawa, 2017.

[15] MEN, "Bezpieczna Szkoła. Procedury reagowania w przypadku wystąpienia wewnętrznych i zewnętrznych zagrożeń fizycznych w szkole" (Safe School. Response procedures in the event of internal and external physical threats in the school), https://bezpiecznaszkola.men.gov.pl/wp-content/uploads/2017/09/procedury-reagowania-w-przypadku-wystapienia-wewnetrznych-i-zewnetrznych-zagrozen-fizycznych-w-szkole-1.pdf, Warszawa 2017.

[16] MEN, "Bezpieczna Szkoła.Działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego" (Safe School. Response procedures in the event of internal and external physical and digital threats in the school), http://bezpiecznaszkola.men.gov.pl/wp-content/uploads/2017/09/zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizycznego-i-cyfrowego-uczniow.pdf, Warszawa 2017.

[17] MEN, "Bezpieczna Szkoła.Kompendium wiedzy dla dyrektora szkoły" (Safe School. A compendium of knowledge for the school head), http://bezpiecznaszkola.men.gov.pl/wp-content/uploads/2017/09/kompendium-wiedzy-dla-dyrektora-szkoly.-1.pdf, Warszawa 2017.

[18] Safe Cyber School, https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach, Warszawa 2020.

[19] M. Tanaś, M. Gajewska-Pol, J. Gursztyn, A. Maj, M. Różycka, A. Rywczyńska, K. Silicki, "Jak zapewnić uczniom bezpieczeństwo w Internecie. Poradnik dla nauczycieli" (How to keep students safe on the Internet. A guide for teachers), https://akademia.nask.pl/pliki/1-jak-zapewnic-uczniom-bezpieczenstwo-w-internecie-poradnik-dla-nauczycieli.pdf, NASK.

[20] K. Majewska, "Sensory Preferences of Teachers in the Context of Computer Educational Tools Using", *Educational Studies Review* no 31 (2/2020), 2020, pp.167-185.

[21] K. Majewska, "Modern educational tools in the teacher's work", *The New Educational Review*, vol. 51, no. 1, 2018, pp. 125-135.

[22] K. Majewska, "Virtual Consumer versus Internet Creator, or Attitudes of Polish Teachers to Online Early School Education. Conclusions for Practice", *The New Educational Review*, vol. 57, no. 3, 2019, pp. 210-222.

[23] K. Majewska, *Nauczanie i uczenie się w przestrzeni mediów wirtualnych (Teaching and Learning in Virtual Media Space)*, Toruń: Wydawnictwo Adam Marszałek, 2021.

[24] D. Siemieniecka, M. Skibińska, "Stalking and cyberstalking as a form of violence", *Society, Integration, Education*, Vol. 3, 2019, Proceedings of the International Scientific Conference, May 24th-25th, 2019, pp. 403-413.

[25] K. Majewska, "Komputerowy sysem egzaminowania" (Computer based examination system), *E-mentor*, vol. 58, no. 1, 2015, pp. 41-47.