Studies in Educational Management

2020 (5) 17–29

Cyberbullying as a Threat to Young

Katarína Kampová*, Katarína Mäkká, Viktor Šoltés

University of Zilina

Received *19 December 2020* ***Accepted*** *25 January 2020*

ABSTRACT

The issue of cybercrime and other anti-social activities is increasingly discussed today. The cause is an increasing number of individuals, companies or states exposed to these threats. This article deals with the issue of cyber aggression as one of the kinds of other anti-social activities. The article presents the results of researches in the Slovak Republic, but also the results of a survey at selected schools conducted by the Faculty of Safety Engineering of the University of Žilina. The main aim of the article is to point out the issue of cybercrime and other antisocial activities among adolescents and to point out the relationship between their education and vulnerability.

Keywords: *Cybercrime, Security, Cyberbullying, Vulnerability, Young People*

Cyberbullying as a Threat to Young

The security and protection of individuals, groups and society from crime and other anti-social activities related to the use of modern information and communication systems and technologies is becoming increasingly challenging not only for Slovakia, the EU but also for other countries in the world. This statement can also be confirmed by the results of recent surveys showing that digital threats are developing rapidly and that the public perceives cybercrime as a significant threat. Up to 87% of respondents regard cybercrime as an important challenge for the EU's internal security (Petranová & Vrabec, 2015). This upward trend is also related to the number of people using the Internet. For an idea 10 years ago, the number of people using the Internet was about

Correspond author E-mail address: katarina.kampova@fbi.uniza.sk

"1.5 billion", but in 2018 it was "... 4.3 billion users". The growth of Internet users is presented in (Figure 1).

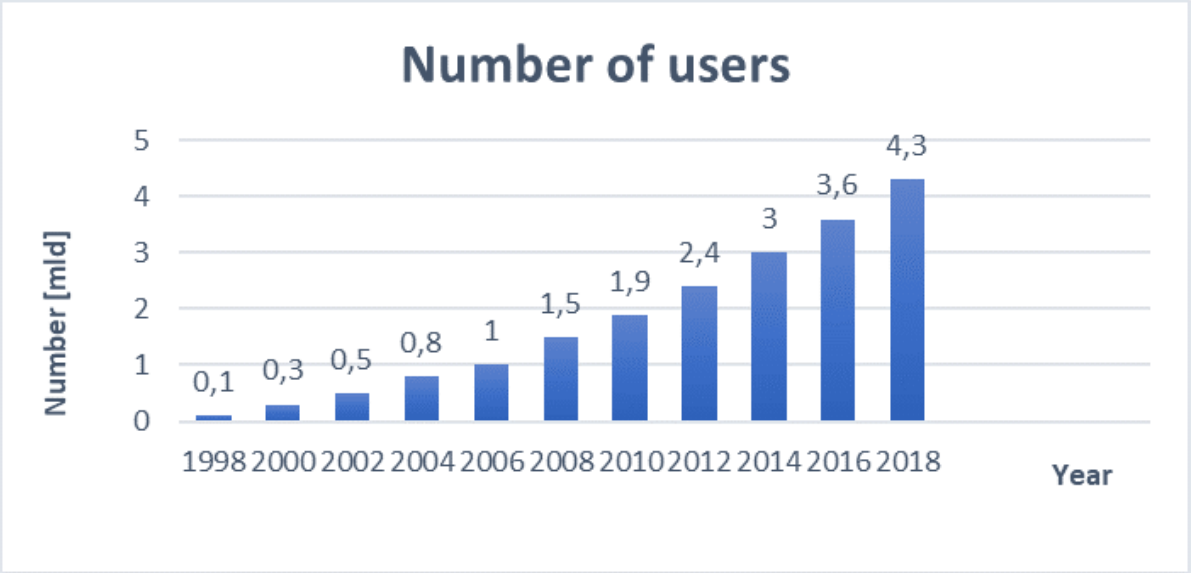

Figure 1. Increase in Internet Usage. (Source: Strategy of prevention of criminal and other antisocial activities in the Slovak Republic for years 2016 – 2020).

Vulnerabilities that arise from this open virtual world, which links the individual entities with each other without unambiguous constraints, create the preconditions for causing various threats (Holla & Hanuliakova, 2016). One of these threats is cyber-aggression or cyberbullying of young persons.

Cyberbullying among juveniles

Bullying was until the 1970s only considered a phenomenon inherited for centuries. Scientists have only begun to investigate it from this time onwards when he noticed his increase among young people and pupils.

In the past, people did not consider bullying to be a problem that would require increased attention. Bullying was taken as part of childhood and adolescence. In the last two decades, the view of bullying has changed and is seen as a serious problem (Shaheen, 2008).

As in the world, the Slovak Republic is not an exception and bullying is a serious threat. Bullying is any behaviour, with the intention of hurting, threatening or intimidating another person, or a group of people. It can have different forms and levels of progress.

Most often it carries elements of psychological coercion and physical harm. The consequences of such behaviour are reflected in mental and physical health and can be serious and lifelong. The basic characteristic of bullying is (Martinek, 2009):

- predominance of strength (physical, mental, mental, quantitative, power). The victim perceives the attack unpleasantly and cannot defend himself,
- mostly repeated and targeted action on a particular individual which is escalating,

- motive to hurt without objective cause based on the aggressive vision of an aggressor who goes beyond social norms,
- the attacker is either an individual or a group,
- the basic feature of the victims is helplessness. The victim cannot or is afraid to seek help from his surroundings.

According to Vágnerová (2004), bullying is a humiliating behaviour of an individual or a group against a weaker individual who is unable to escape from him or to defend himself effectively. Bullying is a manifestation of abuse of status and power that an individual has acquired in a group (Vágnerová, 2004).

Bullying and cyberbullying are dangerous social pathological phenomena in which there is a restriction of personal freedom, freedom of choice, the humiliation of human dignity and honour, and often harm to health or property (Paľovčíková, 2018).

Cyberbullying, as one of the new forms of bullying, is generally defined as a direct form of bullying involving the misuse of information and communication technologies (especially telephone, tablet, internet and social networks) for deliberate threats, harm or intimidation, often occurring in links with other forms of bullying.

One of the basic characteristics of cyberbullying is that it takes place in a cyber environment. This environment defines (Marková, 2018) as a virtual environment that has no boundaries or limitations. It is a global dynamic open system of networks and information systems that consists of activated elements of cyberspace, the people who perform activities in this system, and the relationships and interactions between them (Ristvej, Zagorecki, Hollá, Šimák, & Titko, 2013). We cannot talk about bullying and cyberbullying on occasional exchanges of views. It is usually a long-term process of creating psychological domination over another person, which is often presented externally (Kampová, Mäkká, Zvaková, & Pellowski W., 2018; Lovecek, Ristvej, Sventekova, Siser, & Vel'as, 2016; Lovecek, Ristvej, Sventekova, Mika, & Zagorecki, 2016; Lovecek, Ristvej, Magdolen, & Ondrejka, 2017). The bully often uses the presence of other persons acting as a silent audience to multiply the presentation of his domination and increase the helplessness of the person or group of persons.

As reported by Shaheen (2008), the most common types of cyberbullying are:

- happy slapping,
- flaming,
- harassment,
- sexual harassment,
- phishing,
- impersonation,
- cyberstalking.

Happy Slapping is still seen as a phenomenon. It first occurred in part of London. This is a type of bullying that is committed by combining physical bullying with cyberbullying. This is a type of bullying that is committed by combining physical bullying with cyberbullying (Kopecký & Szotkowski, 2019). The essence of this bullying is that the victim is physically attacked by an individual or a group of individuals, with one of the offenders recording the entire attack on a

camera or telephone (Svetlík & Veľas, 2016). Later, the record is published on various websites and distributed on the Internet. The European Parliament (2007) also defined this phenomenon as publishing photographs of violent scenes captured on a mobile phone on the Internet. These captured photos or videos are later converted into the desired form using various software and then published on the Internet and distributed among peers (Hollá, 2010).

Flaming is a verbal assault and insult to a victim through social networks or other applications for communication in cyberspace. Flaming does not have to be directed in one direction only. The victim is able to defend himself and verbally attacks the perpetrator in defence (Kowalski, Limber, & Agatston., 2008). Sometimes it is a problem to distinguish a flamer from a lesser-known troll. Troll is a person who usually uses arguments to disrupt a discussion and try to provoke conflict. If flaming is done in real-time and space, there is too much chance that ordinary insults and verbal assaults will become physical assaults. In cyberspace, verbal assault often escalates (Holla, 2015).

Harassment is considered a unique type of cyberbullying. It consists of sending repeated text messages or other messages to the victim. This type of bullying occurs more in the victim's private cyberspace. It works through communication between the offender and the victim, where the offender sends tens to hundreds of repeated messages to the victim (Kowalski, Limber, & Agatston., 2008).

Sexual harassment is another type of cyberbullying that occurs just like classic harassment in cyberspace. This form is conditioned by pre-pubertal, hormonal influences and environment. Paľovčíková (2018) defined three categories of sexual harassment: sex harassment and bullying according to gender, unwanted sexual attention, forcing the victim to act in the interests of the perpetrator.

Phishing is a well-known technique of social engineering. When using this type of cyberbullying, the perpetrator sends false information to his victim in the form of text messages or e-mails, while posing as trustworthy. As a result, the victim inadvertently discloses to the perpetrator his personal information, which the perpetrator subsequently misuses (Kowalski, Limber, & Agatston, 2008).

Impersonation or impersonation is another known type of cyberbullying. When impersonating another person, the perpetrator "takes over" the victim's identity, looks like her, uses her name and personal information, even a profile photo. The perpetrator logs in to the social network under her account, where he or she is deliberately deleting photos, commenting on other people's posts inappropriately, or even changing profile data. In this case, it is difficult for the victim to defend and prove that she has not committed it (Kowalski, Limber, & Agatston., 2008).

Cyberstalking, also known as the victim's cyber-persecution, consists of communicating with the victim using technology to persecute the victim, sending the offender with threatening messages (Šoltés, Repková Štofková, Kutaj., 2016). Stalking is seen as an act where the perpetrator pursues an unsuspecting victim. It is important to realize that this form is not so dangerous at first sight, but it brings with it much more threats than just harassment.

Different types of cyberbullying are a difficult stress situation for young people, which can have serious consequences. The child may suffer from various psychosomatic problems. These

difficulties are mainly caused by stress, conflict and traumatic experience, so situations that we often experience in our daily lives are mainly the cause of psychosomatic diseases. Psychosomatic diseases are not diseases that have a predominantly somatic cause in the body- it is not a diseased organ, but the organism manifests itself as symptoms of the disease as if the body was really ill. Conversely, somatic disease can sometimes have psychogenic causes. At that time, long-term stress, unresolved conflicts and recurring traumatic experiences conditioned the development of somatic or mental illness (Lovecek, Ristvej, Magdolen, & Ondrejka, 2017).

The manifestations of such difficulties may be, for example, abdominal pain, headache, sleep disturbances, experiences feelings of shame, sadness, depression, anxiety or his own failure, but also feelings of constant danger. Cyberbullying may result in his complete psychological collapse and, in the worst cases, suicide (Cañas, Estévez, Marzo, & Piqueras, 2019).

The longer such conditions persist, the more they exhaust the mental and physical resources of the person. This means that the longer the cyberbullying lasts, the more support and assistance the person will need (Informačné centrum Mladých, 2013). Electronic bullying undoubtedly also has social consequences. This may include, for example, loneliness, absence from school, social isolation, impaired learning outcomes, escape from home, use of various substances, or social anxiety or refusal of social communication (Hollá, 2013).

Method

In 2019, a survey was carried out at selected secondary schools by the Faculty of Safety Engineering, University of Žilina in Slovakia. Respondents were students of secondary schools specializing in IT and students of general secondary schools.

The survey sample consisted of 300 respondents, secondary school students focused on general and technical specialization. 59.5per cent of men and 40.5per cent of women participated in the survey. The questionnaire was designed to answer relevant survey questions:

- Are social networks the most common form of cyberbullying in both schools?
- Are the victims' sex related to being victims of cyberbullying?
- Cyberbullying programs encourage students to trust others?
- Is education related to the fact that students are less likely to be victims of this cyberbullying?

The questionnaire contained 13 questions that create the prerequisites for obtaining answers to the main survey questions. In the questionnaire we asked respondents about:

- Respondent's gender.
- The average time they spend daily on the Internet.
- Knowledge of the threat of cyber bullying.
- Whether the student was a victim of cyber bullying.
- If yes, in what form and type the cyberbullying took place.
- If they have been the victim, whether they have confided in someone (parent / teacher).
- Knowledge of the occurrence of cyber bullying at their school.
- If yes, the number of cyberbullying cases at their school.

- What form of cyberbullying occurred at their school?
- Whether cyberbullying prevention program and its form (subject / lectures / other) are included in their school education.
- If yes, in what form is implemented.
- Whether students think cyber bullying is dangerous.
- Whether students protect themselves from the potential threat of cyberbullying.

The nature of the answers to the questions asked was closed and semi-closed. It took about 5 - 10 minutes to complete the questionnaire. Distribution of questionnaires in schools was provided by Faculty of security management University of Žilina experts. The data collection used classical printed questionnaires on paper, which were more suitable for this research than the currently preferred electronic questionnaire. The advantage was also the possibility to keep the respondents' attention and to answer their questions in case of doubt.

Results

The first main question of survey consisted of whether social networks were the most common form of cyberbullying in both schools. The survey found that most cyberbullying cases at both schools were carried out through social networks. There were 30per cent of cases at secondary school with general specialization and 34per cent of cases of cyber bullying committed through social networks.

The second question focused on the connection of respondents' sex with the fact that they are the victims of cyberbullying. The results of the survey do not confirm the assumption that gender is related to possible cyberbullying. In the survey we found that there was approximately the same number of victims based on sex at the school with general specialization, namely 16per cent of male victims and 14per cent of female victims whereas the sample of respondents consisted of 58per cent men and 42per cent women. At the school with technical specialization, the number of victims was much lower. Of all 77per cent of male and 23per cent female respondents in the technical school, was 12per cent male victims and only 3per cent were female victims. This fact has not been confirmed in the survey and the gender has no connection with the fact that the student was bullied.

The third question was about students telling someone that they were being bullied if a cyberbullying prevention program was included in their teaching. The survey found that only 30per cent of cyberbullying victims attending high school with general specialization told someone they were bullied. Up to 57per cent of the victims reported it at the technical school. This difference may be related to the absence of preventive programs at the general secondary school.

The fourth question focused on preventing cyberbullying. Up to 42per cent of general focused secondary school students said that they did not protect themselves against the threat of cyberbullying. Only 9per cent of respondents are not protected at the technical school. As a result, students in this field of study are more vulnerable and sometimes cannot defend themselves.

However, the survey also looked at the dependence between technical education within information technology and its preventive nature regarding cyberbullying and its effects. Survey

results show that these students spend an average of two hours more time on the Internet compared to students of school with general education. The reason for the increased need for spending time on the Internet by technical school students was to meet their study needs.

Based on the evaluation of the students' answers, we can say that students of secondary schools, which have only a general specialization, are worse off when it comes to preventing cyberbullying. There were 15per cent more victims at the generally secondary school than at a technical school and one of the reasons may be that up to 42per cent of the general secondary school students surveyed do not protect themselves from the threat of cyberbullying while only 9per cent students of technical school do not protect themselves. The survey found that only 9per cent of respondents do not protect themselves from cyberbullying in technical schools. 33per cent of these school students often change their passwords, 22per cent watch out with whom they are friends, 32per cent watch out with whom they share information, and the remaining 4per cent of the students indicated another option.

For example, they mentioned 2-step authenticator or that they don´t have much information about themselves on the internet. On the other hand, up to 42per cent of general secondary school students surveyed do not protect themselves from the threat of cyberbullying. 32per cent of interviewed students often change their passwords, 15per cent pay attention to who they have in their friends' list, and the remaining 11per cent pay attention to who they share their personal information with.

Electronic bullying is a modern phenomenon that allows for further information-communication technologies expanding. It is therefore undoubtedly important to emphasize the need to increase effective coping strategies for cyberbullying.

Discussion

A survey conducted by the Faculty of Safety Engineering revealed results analogous to those listed below. In the years 2013 - 2015, research was carried out in the Slovak Republic on a sample of 1619 respondents aged 11 to 18 years. The main aim was to determine the prevalence of cyberbullying. In terms of prevalence, false information and vulgar and offensive comments were most prevalent (Hollá 2017). The overall results are presented in Figure 2.

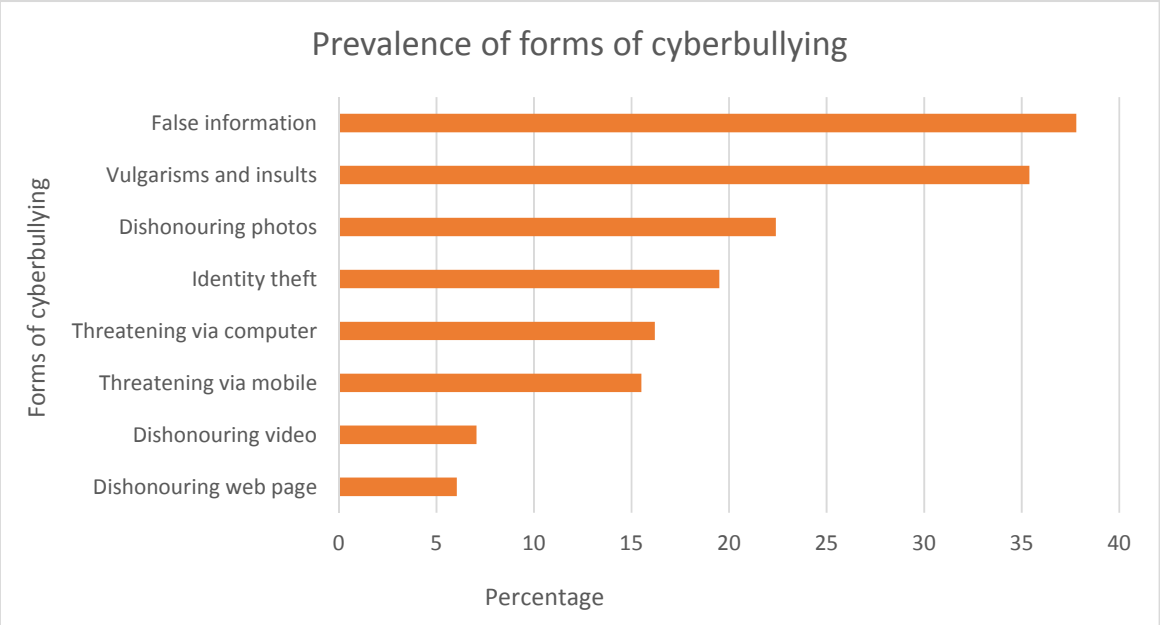

Figure 2. Prevalence of forms of cyberbullying. (Source: Holla, 2016).

Other prevalence data include deforestation photos, identity theft, threats via a computer or mobile phone. The Slovak National Center for Human Rights conducted research on bullying and cyberbullying in schools, which was carried out in 2017/2018. Survey shows that more than half of respondents reported bullying at school (51.8 per cent). Primary school pupils (56 per cent) reported the highest incidence of bullying, but nearly 51 per cent of eight-year high school students and 44.8 per cent of secondary school students also encountered it. Only 9.5 per cent of respondents stated that bullying never occurred at the school they attend.

Pupils in schools in Slovakia have rarely encountered cyberbullying, but according to the results, more than one-third of respondents currently have experience with this phenomenon. 66.3 per cent of pupils have already heard about cyberbullying in cyberspace. More than a third of respondents, 34.9 per cent, have been victims or witnesses of cyberbullying.

Cyberbullying studies among juveniles have confirmed the results of other studies and research. This socio-pathological phenomenon is now becoming widespread and can be said to is becoming a common phenomenon. Bullying and cyberbullying among juveniles cannot be undermined or tolerated. The rapid development of information technology and the increase in intolerance in all areas of society's life require experts to further deepen their knowledge and qualitatively explore the issue of bullying and cyberbullying throughout the context.

In addition, the information technology skills of juveniles also play an important role in preventing cyberbullying. This claim may be justified by the results of a survey aimed at comparing the vulnerability of minors at different levels of education in this area.

As Hollá, K. et.al (2017) states, the best way to tackle bullying is to try to prevent it from happening, and one way to do this is to teach students to work with information technologies so that they can resist these modern threats themselves. According to the European Charter for Media

Literacy (2006), the media literate should be able to identify, prevent, or reject media content and services that may be unwanted, offensive, offensive, and harmful. Media literacy is enhanced information and communication skills and can be classified as one of the most basic life skills in the 21st century (Vrabec & Petranová, 2015).

As mentioned, one of the most important factors influencing the current development of society is the unstoppable development of new information technologies. It can be also stated that we do not find any other significant factor currently affecting the development of new negative social phenomena such as the information technologies mentioned above. Among these new negative social phenomena we can mention in particular the attack from reality into the virtual world of information technologies, abuse of the anonymity of the virtual commutation environment, for example in the case of juvenile bullying.

As stated by Drobný Miro (Public Health Authority of the Slovak Republic, 2015), the primary role of teachers, parents, and other responsible persons in the youth education process is to teach children how to protect themselves in this virtual environment. Here are four principles of cyberbullying protection:

- Disclosure of personal information, photos and videos
- Immediate reaction
- Retention of evidence and removal of pages
- Blocking and reporting cyberbullying.

Young people should know that, as in everyday life, they will not reveal anything about themselves to anyone else, so it should also apply on the Internet. For example, they should learn how to set up access to personal data only to friends, how to choose the correct password, and securely store all documents on the Internet.

Cyberbullying must be addressed immediately. The longer you leave the situation, the worse it can get and the consequences can be more severe. It is essential to teach young people to respond adequately to situations with which they are not satisfied. It is important that they give the perpetrator a strong and unequivocal indication that they are obstructing his/her behaviour and want from him/her to stop it and, if he/she does not, they take further action.

It is necessary to teach the youth that whatever activity in the virtual space remains in it. These clues can serve either to identify the perpetrator or to provide evidence. It is essential to teach children to keep any evidence (for example SMS, e-mail, etc).

Even on the Internet, you can choose who you want to communicate with and who you don't. In both email and chat communication, it is possible to set blocking of messages from the bully.

As Hollá, K. et.al (2017) states, the best way to tackle bullying is to try to prevent it from happening, and one way to do this is to teach students to work with information technologies so that they can resist these modern threats themselves. According to the European Charter for Media Literacy (2006), the media literate should be able to identify, prevent, or reject media content and services that may be unwanted, offensive, offensive, and harmful. Media literacy is enhanced information and communication skills and can be classified as one of the most basic life skills in the 21st century (Vrabec & Petranová, 2015).

A secure environment and ensuring the prevention of bullying and cyberbullying not only in the school environment requires the collaboration of teachers, various other collaborating professionals and parents (Paľovčíková, G. a kol). In addition to increasing the education of children and youth in the field of information technology, it is necessary to deepen the knowledge of parents about the prevention of aggression of children and youth within the cyberspace. It should also be noted that raising public awareness in this area also plays very important role.

Preventing unwanted phenomena related to the use of computer and Internet technologies is not easy and certainly not a one-off process. Within the Slovak Republic, a three-stage prevention model has been created, where individual tasks are solved at national, regional and local levels (Hollá, K. et.al, 2017). Cooperation and synergy between individual regulations and activities of central authorities, state and non-profit organizations, churches, schools and school facilities and, last but not least, families is an important element in the prevention of cyber aggression and cyberbullying in the Slovak Republic.

Main entities are individuals, individual groups and organizations that can successfully contribute to the prevention of cyberbullying. According to (Holla, 2012) at school level, the approach to preventing cyberbullying is based on the education of school staff, students but also parents.

With such an approach it is possible to anticipate, plan, prepare and educate students, cyberbullying workers, but also to provide professional information to parents. The model itself is made up of three processes: planning, prevention and innovation, and case reporting (Holla, 2012). As part of the planning process, it is essential to create a team of people who are involved in preventing bullying in schools. An important task is to innovate and expand the competencies of this team to aim the risks of cyberbullying.

At this stage of the cyberbullying prevention process, it is important to follow these steps: to familiarize school staff with cyberbullying, its manifestations, forms, consequences as a sociopathological phenomenon. To map the occurrence of bullying and cyberbullying at school. The next step is to set up prevention and intervention programs, which involves collecting resources, activation techniques and methods, and drawing up disciplinary measures.

In the second stage of prevention and innovation, awareness of cyberbullying is an important task. Many teachers, students and parents are unaware of the dangers associated with the electronic media, therefor education and information are an essential part of preventing cyberbullying. This level creates conditions for raising awareness of cyberbullying through cyberbullying, by developing practices and interventions through training, activities and exercises that emphasize basic human values, develop empathy in relation to the issue. Sanctions must be also provided for at this stage. The school policy should clearly define the possibilities of using technology in schools and their space.

The third stage of Case Reporting consists of setting up a system for reporting individual cases and dealing with these cases. The third stage of Case Reporting consists of setting up a system for reporting individual cases and dealing with these cases.

The model represents one of the possible ways of preventing cyberbullying in schools. There are many other approaches in the literature that also create preconditions for reducing this phenomenon (Jadambaa, Thomas, Scott, Graves, Brain, & Pacella, 2019).

The role of parents in the cyberbullying prevention process is to accept the fact that the virtual world belongs to the lives of children and young people and to teach or create conditions for them to move safely in this environment (Betts, 2019).

Cyberbullying studies among juveniles have confirmed the results of other studies and research. This socio-pathological phenomenon is now becoming widespread and can be said to is becoming a common phenomenon. Bullying and cyberbullying among juveniles cannot be undermined or tolerated. The rapid development of information technology and the increase in intolerance in all areas of society's life require experts to further deepen their knowledge and qualitatively explore the issue of bullying and cyberbullying throughout the context. In addition, the information technology skills of juveniles also play an important role in preventing cyberbullying.

References

Boroš, M., Kutaj, M., Mariš, L., & Veľas, A. (2018). *Development of Security at the Local Level through Practical Students Training*. Paper presented at the 12th International Technology, Education and Development Conference, Valencia, Spain.

Cañas, E., Estévez, E., Marzo, J. C., & Piqueras, J. A. (2019). Psychological adjustment in cybervictims and cyberbullies in secondary education. *Anales de Psicologia, 35*(3), 434–443.

Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research, 14*, 206–221. http://dx.doi.org/10.1080/13811118.2010.494133

Hollá, K. (2010). *Elektronické šikanovanie – nová forma agresie* [Electronic bullying - a new form of aggression]. Slovakia: IRIS.

Holla, K. (2012). *Kyberšikana: prevence a intervence jako aktuálni výzva pro školy* [Cyberbullying: prevention and intervention as a topical challenge for schools]. Paper presented at the Evropské pedagogické fórum 2012, Hradec Kralove, Czech republic.

Holla, K. (2015). Cyberbullying as a negative result of cyber-culture of Slovak childeren and adolescents:selected research findings. *Journal of Language and Cultural Education, 4*(2), 40–55.

Holla, K., & Hanuliakova, J. (n.d.). Social positions of students and cyberbullyning. *Ad Alta- Journal of Interdisciplinary Research, 7*, 52–57.

Hollá, K., Jedličková, P., Fenyvesiová, L., Hanuliaková, J., Határ, C., & Kurincová, V. (2017). *Prevencia kyberagresie a kybesikanovania* [Prevention of cyberagression and cyberbullying]. Nitra, Slovak republic: DMC, s.r.o.

Informačné centrum Mladých. (2013). *Kyberšikana, nebezpečenstvo v elektronickej podobe* [Brochure]. Retrieved from http://www.icm.sk/subory/Kybersikanovanie.pdf

Jadambaa, A., Thomas, HJ., Scott, JG., Graves, N., Brain, D., & Pacella, R. (2019). Prevalence of traditional bullying and cyberbullying among children and adolescents in Australia: A systematic review and maeta-analysis. *Australian and New Zealand Journal of Psychiatry, 53*(9), 878–888.

Kampová, K., Mäkká, K., Zvaková, Z., & Pellowski, W. (2018). *The eSEC Portal as a Tool for the Concept of Corporate Social Responsibility*. Paper presented at the 16th International Conference on Emerging Elearning Technologies and Applications, High Tatras, Slovakia.

Kopecký, K., & Szotkowski, R. (2019). *České děti v kybersvětě* [Czech children in the cyberspace]. Retrieved from Centrum prevence rizikové virtuální komunikace website: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/117-ceske-deti-v-kybersvete/fil

Kowalski, RM., Limber, SP., & Agatston, PW. (2008). *Cyber Bullying*. Oxford, England: Blackwell Publishing.

Lovecek, T., Ristvej, J., Sventekova, E., Siser, A., & Vel'as, A. (2016). Currently Required Competencies of Crisis and Security Managers and New Tool for Their Acquirement. Paper presented at the 3rd International Conference on Management Innovation and Business Innovation, Manila, Philippines.

Lovecek, T., Ristvej, J., Sventekova, E., Mika, VT., & Zagorecki, A. (2016). *Currently Required Competencies of Crisis and Security Managers and New Tool for their Acquirement – The eSEC portal*. Paper presented at the 13th IEEE International Conference on Emerging eLearning Technologies and Applications , 2016, Slovakia.

Lovecek, T., Ristvej, J., Magdolen, M., & Ondrejka, R. (2017). *Determination of Personal Data Sensitivity and Security Measures Assignment*. Paper presented at the International Conference on Management Science and Management Innovation, Suzhou, China.

Marková, V. (2018). *Súčasný stav a východiská počítačovej kriminality* [Current state and bases of cybercrime]. Paper presented at the Conference Current challenges of cybercrime prevention, Bratislava, Slovakia. Abstract retrieved from https://www.akademiapz.sk/sites/default/files/KIM/ZBORN%C3%8DK%2021.3.2018%20WEB_0.PDF

Martinek, Z. (2009). *Agresivita a kriminalita školní mládeže* [Aggressiveness and criminality of school youth]. Praha: Grada Publishing.

Oster, J. (2017). Cyber crime and its prevention in school environment. Retrieved from http://preventista.sk/info/pocitacova-internetova-kriminalita-a-jej-prevencia-v-skolskom-prostredi/

Paľovčíková, G. (2018). Bullying and cyberbullying in schools. Retrieved from http://mladez.sk/wp-content/uploads/2019/01/%C5%A0ikana_a_kyber%C5%A1ikana_2018.pdf

Paľovčíková, G., et al. (2018). *Šikana a kyberšikana na školách* [**B**ullying and cyberbullying in schools] (ISBN: 978-80-89016-99-0). Retrieved from Slovenské národné stredisko pre ľudské práva website: http://mladez.sk/wp-content/uploads/2019/01/%C5%A0ikana_a_kyber%C5%A1ikana_2018.pdf

Petranová, D., & Vrabec, N. (2015). *Mediálna gramotnosť dospelej populácie v SR* [Media literacy of the adult population in Slovakia]. Retrieved from https://issuu.com/medialnavychova.sk/docs/medialna_gramotnost_dospelej_popula

Public Health Authority of the Slovak Republic. (2015). *Predchádzajme kyberšikane* [Brochure]. Retrieved from http://www.uvzsr.sk/docs/info/podpora/letaky/kybersikanovanie.pdf

Ristvej, J., Zagorecki, A., Hollá, K., Šimák, L., & Titko, M. (2013). *Modelling, Simulation adn Informatin Sstems as a Tool to Support Decision-Making Process in Crisis Management*. Paper presented at the European Simulation and Modelling Conference, Lancaster, United Kingdom.

Shaheen, S. (2008). *Cyber-bullying – Issues and solutions for schools, the classroom and home.* Oxford, England: Routledge.

Šoltés, V., Repková Štofková, K., & Kutaj, M. (2016). *Education as a regional development aspect*. Paper presented at the EDULEARN16: 8TH International Conference on Educationand New Learning Technologies, Barcelona, Spain.

Stratégia prevencie kriminality a inej protispoločenskej činnosti v Slovenskej republike na roky 2016-2020 [Summary of the Strategy of prevention of criminal and other antisocial activities in the Slovak Republic for years 2016 - 2020]. (n.d.). Retrieved from Ministry of Interior of the Slovak Republic website: https://www.minv.sk/?zakladne-dokumenty-rvpk

Stratégia prevencie kriminality a inej protispoločenskej činnosti v Slovenskej republike na roky 2016-2020. [Summary of the Strategy of prevention of criminal and other antisocial activities in the Slovak Republic for years 2016 - 2020]. (n.d.). Retrieved from Ministry of Interior of the Slovak Republic website: http://www.minv.sk/?zakladne-dokumenty-rvpk

Svetlík, J., & Veľas, A. (2016). *The Safety Training in The Municipality.* Paper presented at the Edulearn16: 8th International Conference on Education and New Learning Technologies., Barcelona, Spain.

Vágnerová, M. (2004). *Psychopatologie pro pomáhajícíprofese: variabilita a patologielidské psychiky*. Prague, Czech Republic: Praha portál.

Vrabec, N., & Petranová, D. (2015). Koncepcia kybernetickej bezpečnosti na roky 2015-2020. Retrieved from http://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Konce_pcia--bezpe_cnosti-SR-na-roky-2015-2020-A4.pdf