Received: 28.01.2021.
doi: 10.46763/JESPT211610047an
udc: 37.018.43:004]-049.5
Revised: 19.02.2021.
Accepted: 05.03.2021.

SAFE TEACHING FOR SAFE EDUCATIONAL INSTITUTIONS – ISTHERE THE HIDDEN CRISIS?

Marija Apostolova Nikolovska[1]

Government of the Republic of N. Macedonia,
marija.apostolova@primeminister.gov.mk

Abstract. Education is the cornerstone of development of each country and is recognized by the UN as a human right. Access to safe learning environments is a vital requirement at every stage of child's education – from the preschool, during which a child's brain undergoes 90% of its development, through to adolescence, when young people are prepared for the contributions they will then make to their communities, the economy and the wider world. This paper instigate many questions for safe teaching: What do the data tell us about violence and cyberbullying? How can educational institutions counterbalancing this "situation"? Also is pointed, that no country can achieve inclusive and equitable quality education for all, if students experience violence and cyberbullying in educatonal institutions and beyond.A quality education can improve the life chances of individuals themselves, especially to girls and the communities around them. The purpose of this paper is not to analyze the proposed solutions for online teaching in terms of cyber security and protection of studentprivacy, but must point out a number of potential risks that the process itself carries. Namely, the lack of unified access to online teaching in the period March-June 2020 has led to almost every school collecting, storing and transferring personal data of students to a variety of software and web services. At the beginning of the new school year, it was start a single platform is used for all schools, and therefore competent institutions must to pay attention to data security and to respect the principles of privacy of children. This paper also raises the question what is the effect on children in this digital migration? The paper states that competent institutions need to have a macro and micro approach in order to provide a safe learning environment.

Key words: *cyberbullying, hidden crisis, development, safe educational institutions.*

Introduction

Preventing a learning crisis from becoming a generational catastrophe requires urgent action from all. Education is not only a fundamental human right, it is an enabling rightwith direct impact on the realization of all other human rights. It is a global common goodand a primary driver of progress across all 17 Sustainable Development Goals as a bedrockof just, equal, inclusive peaceful societies. When education systems collapse, peace, prosperous and productive societies cannot be sustained.

The COVID-19 pandemic and the physical distancing measures imposed in responseto it have greatly increased the risk of intra-family violence and online abuse. New researchs reveal the sheer scale of the challenge and the impact of inaction on school safety. In the executive summary of the report „Safe schools: the hidden crisis - A framework for action to deliver Safe, Non-violent, Inclusive and Effective Learning Environments" (Brown, 2018), it is pointed that within two years, there will be an estimated 550 million children of school and pre-school age (3–18), living across 64 countries, whose education is under threat from war, endemic high violence, or environmental threats. At the same time, it is emphasized that by 2030, this number will rise to 622 million – nearly a third of all children that will be alive at that point and the projections are grim: nearly a quarter of these children (22%) will not complete primary school, over half (54%) will not complete secondary school, and three-quarters (75%) will fail to meet basic learning outcomes in literacy and maths. These percent starkly show, failure to improve the safety of schools in the countries that are part of this report makes realizing

the ambitions set out in the UN's Sustainable Development Goals on education (SDG4) impossible. In parallel, denying these children the education they deserve risks depriving some of the world's most challenging areas of entire generations of builders, producers, innovators, problem-solvers, peace-makers, entrepreneurs, careers and life-savers.

A range of objectives relating to global education to be achieved by 2030 are: providing safe, non-violent, inclusive and effective learning environments for all, ensuring that all girls and boys complete free, equitable and quality primary and secondary education leading to relevant and effective learning outcomes, ensuring that all girls and boys have access to quality early childhood development, care and pre-primary education so that they are ready for primary education and eliminating gender disparities in education and ensuring equal access to all levels of education and vocational training for the vulnerable, including persons with disabilities, indigenous peoples and children in vulnerable situations.

Need for safe educational institutions

Safe educational institutions and learning environments (also called 'safe learning spaces') are physical locations or ways in which young people can learn free from systematic threats to the physical and mental wellbeing of themselves and their teachers. They are places where the physical infrastructure is also safe for learning (Dweck, 2008). Threats to safe schools exist in every country in the world. However, they are inevitably heightened in countries affected by conflict, environmental disasters, and high levels of endemic violence. The known disruption caused to their education - pre-school, primary, secondary and beyond is immense: it is estimated that some 75 million children and youth will have their education disrupted this year due to an emergency or crisis. In the article - Creating the safe learning environment, Timothy C. Clapper emphasized that learning, involves ongoing reflection by the learners as they work to add to or modify the existing frames of reference that they came into the learning environment with (Clapper,2010). For children, this involves being free to take such risks without being mocked in the classroom,or even later, outside the classroom. The UN and the education community have developed guidance (UNESCO, 2020) to help countries through the timing, conditions, and processes for reopening education institutions. Based on an extensive review of existing conceptual frameworks that UNESCO has identified nine key components (UNESCO, 2019) of a response for ending school violence and bullying. These components are the following: strong political leadership and robust legal and policy framework to address school violence and bullying, training and support for teachers on school violence and bullying prevention and positive classroom management, curriculum, learning & teaching to promote, a caring (i.e. anti- school violence and bullying) school climate and students' social and emotional skills, a safe psychological and physical school and classroom environment, reporting mechanisms for students affected by school violence and bullying, together with support andreferral services, involvement of all stakeholders in the school community including parents, student empowerment and participation, collaboration and partnerships between the education sector and a wide range of partners (other government sectors, NGOs, academia).

Defining term „cyberbulling"

UNESCO member states declared the first Thursday of November 5 2020 for International day against violence and bullying at school including cyberbullying and in report of UNESCO (UNESCO, 2020) it is pointed that school violence and bullying including cyberbullying is widespread and affects a significant number of children and adolescents. Cyberbullying includes being bullied by messages, i.e. someone sending mean instant messages, postings, emails and text messages or creating a website that makes fun of a student or by pictures, i.e. someone taking and posting online unflattering or inappropriate pictures of a student without permission; it also refers to being treated in a hurtful or nasty way by mobile phones (texts, calls, video clips) or online (email, instant messaging, social networking, chatrooms) and online hurtful behaviour (UNESCO, 2019).

Relevant research - What do the data tell us about violence and cyberbullying?

EU-level surveys say that 1 in 3 internet users is a child and even half of children aged 11-16 meet with one of the most common risks on the internet4 such as cyberbullying, cyber-predators, scams, malware, fishing (phishing). On the other hand, the same research shows that more half of the respondents do not know how to deal with it the dangers of the internet (European Commision, 2020).

The publication - Behind the numbers ending school violence and bulling, provides an up-to-date and comprehensive overview of global and regional prevalence and trends related to school-related violence and examines the nature and impact of school violence and bullying. In this publication it is pointed that Cyberbullying affects as many as one in ten children. In Europe, girls (11.7%) are slightly more likely to experience cyberbullying via messages than boys (9.3%), whereas boys (8.1%) are slightly more likely to experience cyberbullying via pictures than girls (7.5%). Relatively few case study countries provide data on cyberbullying or strategies to address it. Only two countries, Italy and Lebanon, report teacher training on online safety and prevention and reporting of cyberbullying (UNESCO, 2019).

In the report - Catching the virus; cybercrime, disinformation and the COVID- 19 pandemic published on April 3 2020, Europol pointed that Offenders are likely to attempt to take advantage of emotionally vulnerable, isolated children. It is pointed that children allowed greater internet access and they will be increasingly vulnerable to exposure to offenders through online activity such as online gaming, the use of chat groups in apps, phishing attempts via email, unsolicited contact in social media and other means (EUROPOL, 2020). Adults working remotely subsequently are not as able to supervise their children's internet activity. The report states that cybercriminals have been among the most adept at exploiting the COVID-19 pandemic for the various scams and attacks they carry out and activity around the distribution of child sexual exploitation material online appears to be on the increase, based on a number of indicators.

On April 4 2020 the UK's National Crime Agency published its threat assessment and that "it believes there are a minimum 300,000 individuals in the UK posing a sexual threat to children, either through physical 'contact' abuse or online." The report continued and highlighted that "with children spending more time online to do school work or occupy themselves while parents and carers are busy, they face an increased threat from offenders who are also online in greater numbers", "urging children, parents and carers to ensure they know how to stay safe on the web" (UK's National Crime Agency, 2020).

Cyberbullying is a growing problem. Data from seven countries in Europe show that the proportion of children aged 11-16 years who use the Internet and who had experienced cyberbullying increased from 7% in 2010 to 12% in 2014 (UNESCO,2019).

In the education report - Digital Education: The cyberrisks of the online classroom itis pointed that , in June 2020, Microsoft Security Intelligence reported that the education industry accounted for 61 percent of the 7.7 million malware encounters more than any othersector (Kaspersky, 2020). Apart from malware, educational institutions were also at increasedrisk of data breaches and violations of student privacy. As fall approaches, digital learning will continue to be a necessity. From the end of April to mid-June, Check Point Research discovered that 2,449 domains related to Zoom had been registered, 32 of which were malicious and 320 of which were "suspicious". Suspicious domains were also registered for Microsoft Teams and Google Meet. In 2020, however, the total number of users that encountered various threats disguised as popular online learning platforms jumped to 168,550, a 20,455% increase.

The growing popularity of digital services in education will also contribute to the demand for cybersecurity. After working with distance learning, teachers, principals and parents must to realized the importance of digital security. It is now up to the industry to introduce digital security lessons for teachers, so that they can pass on new knowledge and skills to their students.

Safe teaching in macedonian education: How can educational institutions counterbalancing this "situation"?

Macedonian education also confronted with increased opportunity for digital technology's potential for misuse - from cyberattacks and crimes to misinformation, as wellas burgeoning issues related to data privacy and security. In Macedonia, the models for the beginning of the new school

2020/2021 year that were mentioned during july and august metwith great reactions from the public. SONK issued a statement saying that the priority of the authorities should be the health of students as well as employees, hoping that the proposed models will reflect these values (SONK, 2020). Representatives of the Union of High School Students of the Republic of N. Macedonia also expressed their opinion, saying that "the health, safety and well-being of the school community must be at the center of the policiesfor returning to school." (Union of High School Students of the Republic of N. Macedonia, 2020).

Protecting the safety of children is crucial to the success of the whole reform, whichis based on the advancement of a range of basic human rights as well as internet addiction. Facing these risks should begin with their involvement in the debate, the result of which will be the future strategic documents that will be a framework for organizing distance education.The data from the State Statical Office show that 2020 in Macedonia 79.9% of the households had access to the Internet at home and the most the Internet is used by young people aged 15 to 24 years, for instant messaging, messaging for example, via Skype, Messenger, Whats App, Viber (95.8%) and 89 % participating in social networks (creating user profile, posting messages or other contributions to Facebook, Twitter, etc.) (State, Statistical Office, 2020).

Social media and the many opportunities it offers the internet is a landmark of the 21st century. Cyberbullying is real problem of today, and the victim can be anyone, especially young people. The scandalous group "Public Room" at Telegram came to life again after a year. After months, at least ostensibly, of stopping the activities of members of the group who publicly harassed and published explicit photos of underage girls, these days the public is upset again, after some of the victims alerted to new abuses. The Telegram Public Room group has more than 6,500 members and about 10,000 photos and videoshave been shared. The interior ministry in Macedonia is investigating who is behind thegroup and is urging citizens to report abuses.

UNICEF in the article Cyberbullying: What is it and how to stop it? emphasizes that the laws against bullying, and especially against cyberbullying, are quite new and have not yet been enacted in all countries (UNICEF, 2020). Therefore, a large number of countries, including Macedonia, must support other laws, such as those intended to protect children from all forms of violence and discrimination, including cybercrime. However, in accordance with Article 144, paragraph 4 of the Criminal Code in Macedonia, it is said that on the basisof an information system be threatened with a sentence of five years imprisonment (Criminal Code, 2020). Also, according to the law, anyone who posts private videos on the Internetwith pornographic content may be held accountable for the crime of misuse of personal data under Artcle 149 of the Criminal Code, which carries a fine or up to one year in prison. If the videos show a minor, the perpetrator who produced child pornography for the purpose of its distribution, or transmitted or offered it through a computer system, will be responsible for production and distribution of child pornography Article 193-a of the Criminal Code for which overdue imprisonment of at least eight years. Civil society representatives say they will insistthat sexual harassment online be specifically regulated in the Criminal Code.

Bearing in mind that the threat made through social networks is as important as any other form of threat, it should not be ignored and should be reported to the nearest police station. Before reporting the case to the police, the victim should be sure to hear a copy (screenshot) of the communication as well as a copy (screenshot) of the suspect's profile as evidence that he was present at the time, in case it was too late to remove it. In addition, the class teacher and the professional service in the school should be informed, who would act accordingly in the given situation.

In 2018, the National ICT Council adopted the National Cyber Security Strategy 2018-2022 and the Open Data Strategy 2018-2020 with an Action Plan. The National Cyber Security Strategy of the Republic of Macedonia is a strategic document that should serve as a roadmap for the development of safe, secure, trusting and resilient digital environment, supported by quality capacities based on trust and cooperation in the field of cyber security. The Center for Research and Policy Making in 2019 (Cekov, 2019) has developed a Guide for Cyber Security for Children at Home and School. This publication has been producedwith the support of the City of Skopje, Hedaja - Center for Excellence in Dealing with Violence extremism and the European Union. This guide aims to develop guidelines for

proper use of the Internet that will be readable and practical for teachers, parents and children for the same to be easy applicable.

In July 2020, the Ministry of Education and Science published a Concept for thedevelopment of a distance education system in primary and secondary schools in theRepublic of N. Macedonia. The draft Concept lists several distance learning platforms, someof which are owned by the BDE, some of the relevant ministries, while in practice in the past 4 months many schools have used other platforms (Zoom, Google Classroom, Moodle, etc.).The recording of classes, as well as all the data required for the use of different platforms, in accordance with the European GDPR regulation to which our legal systemadapts, is often treated as the transfer of personal data to other countries. For this, the lawsrequire informing the parents, and even their consent. For schools, this can be an additional administrative burden, for which additional resources should be provided, in order to ensure a uniform practice in the use of data in all schools. The document itself indicates the need toamend the laws in the field of education, but in the process of changes should care is takenon how the principles of personal data protection of all involved individuals will be respected.It is necessary to define exactly who will be the controller, who will be the processor, andwho will be the user of all that data, to specify the deadline storage, the technical protection measures. In the next period, it is necessary for the competent institutions to promote aculture of cyber security, which means encouraging responsibility and understanding ofcyber risks in all spheres of society, by developing informed trust of users in electronicservices. Achieving this goal means creating skills, knowledge and protection solutions, while providing greater resistance to malicious cyber activities.

In addition, this goal will enable effective dissemination of cyber security measures and activities at all levels, including stakeholders, to achieve the required level of knowledge and skills. On the other hand, it is necessary to develop and promote curricula and trainings in the field of cyber security at all levels, support research facilities and business innovations by creating a scientific research center in the field of cyber security, as well as participationin national and international research projects and activities related to cyber security.

Conclusion

In the next period, educational institutions need to review their cybersecurity programs and adopt appropriate measures to better secure their online learning environments and resources. The health, safety and wellbeing of staff, students in educational institutions must to be is highest priority to the governments.

Competent institutions in Macedonia must realize more activities which will aims to increase children's access to more effective, social-emotional learning and life-skills training, and ensure that school environments are safe. Competent institutions need to have a macro and micro approach in order to provide a safe learning environment. The strategy must involves approaches such as increasing enrolment in pre-school, primary and secondary schools, establishing a safe and enabling school environment and life and social skills training programmes. Programmes that strengthen children's social and emotional learning enhance their communication and relationship skills and help them learn to solve problems, deal with emotions, empathize and safely manage conflict – life skills that can prevent violence.

Schools, universities and the teaching staff in this global crisis need to be very careful with the devices where the personal data of all involved in the teaching process are stored, especially the minors (students), because of the possible consequences and privacy violations that could occur with potential breach of protection. In the next period there is a need for greater involvement of parents in school activities related to ICT such as informativemeetings where families are introduced to the specifics of computerized teaching, resources and tools used, protection of privacy and their safety and the safety of their children. At the same time, it is necessary to provide a program for the Safety of children's rights on the Internet, point out the possible risks, and raise awareness of the possible effects of digital exposure. Also, there is need for trainings in the schools of the psychological-pedagogical staff for detecting and dealing with cyber violence and crime.

It is clear that COVID-19 will have a lasting impact on children, particularly online and consequentially, policies and plans will need to accommodate this. It is necessary to promote awareness of cyber threats and focus on capacity building for cyber security among stakeholders, increase awareness and basic knowledge in the field of cyber security of students in primary and secondary schools, improve existing curricula in primary and secondary schools and inclusion of elements in the field of cyber security in the new university study programs in order to produce better staff in the field of cyber security.

No country in all over the world can't achieve inclusive and equitable quality education for all, if students experience violence and cyberbullying in educational institutionsand beyond.

In addition, the possibility of a hidden crisis will be reduce, if there is exchange of skills, knowledge and experiences in the field of cyber security at the national level and that will be achieved through the creation of ad-hoc inter-ministerial research teams composed ofexperts from the public sector, the private sector and the academic community.

References

Brown, S., (2018). Theirworld report: Safe schools: the hidden crisis - A framework for action to deliver Safe, Non-violent, Inclusive and Effective Learning Environments. Conrad N. Hilton Foundation. Retrieved from: http://s3.amazonaws.com/theirworld-site-resources/Reports/Theirworld-%20Report-Safe-Schools-December-2018.pdf.

Cekov. A., (2019). Guide for Cyber Security for Children at Home and School, Center for Research and Policy Making. City of Skopje, Hedaja - Center for Excellence in Dealing with Violence extremism and the European Union. Retrieved from: http://www.crpm.org.mk/wp-content/uploads/2019/12/Vodich_za_sajber_bezbednost_PRINT.pdf

Clapper, T. C, (2010). Creating the safe learning environment. PAILAL, 3(2), 1-6.

Criminal Code, Retrieved from: https://dejure.mk/zakon/krivichen-%20zakonik

Dweck,C.S.,(2008). The perils and promisis of praise. Educational Leadership, 65.34-39.

Education report, (2020). Digital Education: The cyberrisks of the online classroom, Kaspersky. Retrieved from: https://securelist.com/digital-education-the-cyberrisks-of-the-online-classroom/98380/

Europol, (2020). Catching the virus cybercrime, disinformation and the COVID-19 https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercr%20ime_disinformation_and_the_covid-19_pandemic_0.pdf.

Jensen, E., (2008). Brain-based learning (2d ed.). Thousand Oaks, CA: Corwin Press.

Independent trade union for education, science and culture in Macedonia (SONK). Retrieved from: http://sonk.org.mk/.

MacLean, P. D.,(1990). The triune brain in evolution: role in paleocerebral functions. New York: Plenum Press. https://doi.org/10.1126/science.250.4978.303-a

Ministry of Education and Science. (2020). Concept for the development of a distance education system in primary and secondary schools. Retrieved from: http://mon.gov.mk/stored/document/Koncept-za-dalecinsko-%20obrzovanie.pdf.

National Cyber Security Strategy 2018-2022, Retrieved from: https://www.mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/ns_saj%20ber_bezbednost_2018-2022.pdf.

Senthilkumar, K., & Sathishkumar, E. (2017). A Survey on Cyber Security Awareness Among College Students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering, 263, 1-10. https://doi.org/10.1088/1757-899x/263/4/042043

State Statistical Office. (2020) Usage of information and communication technologies in households and by individuals, 2020. Retrieved from: http://www.stat.gov.mk/pdf/2020/8.1.20.31_mk.pdf.

UNESCO, (2018). Global Education Monitoring Repot. Aid to Education: A Return t o Growth? Retrieved from: http://www.unesco.org/images/0026/002636/263616e.pdf./

UNESCO, Section of Partnerships, Cooperation and Research, Division for Education 2030 Support and Coordination, Unpacking Sustainable Development Goal 4 Education – Guide. 2020. Retrieved from: https://campaignforeducation.org/docs/post2015/SDG4.pdf

UNESCO, (2019). Behind the numbers Ending school violence and bulling, Paris: UNESCO.

UNESCO, UNICEF, WFP, World Bank, "Framework for reopening schools", (2020). available at https://unesdoc.unesco.org/ark:/48223/ pf0000373348 and "Reopening schools: How to get education back on track after COVID-19", 2020, Retrieved from: https://www.google.com/search?q=http%3A%2F%2Fwww.iiep.unesco.+org%2Fen%2Freopening-schools-how-get-+education-back-track-after-covid-19-13424&oq=http%3A%2F%2Fwww.iiep.unesco.+org%2Fen%2Freopening-schools-how-get-+education-back-track-after-covid-19-13424&aqs=chrome.0.69i59j69i58.35474j0j4&sourceid=chrome&ie=UTF-8 See also Global Education Cluster, "Safe back to school: a practitioner's guide", 2020, Retrieved from: https://educationcluster.app.box.com/v/Safeback2schoolGuide.

Union of High School Students of the Republic of N. Macedonia. Retrieved from: https://www.radiomof.mk/sojuz-na-srednoshkolci-nashite-%20aktivnosti-kje-prodolzhat-se-dodeka-site-nashi-baranja-ne-bidat-prifateni/

UNICEF, Cyberbullying: What is it and how to stop it? Retrieved from: https://www.unicef.org/northmacedonia/cyberbullying-what-it-and-how-%20stop-it.

UNODC, (2019). University Module Series - Cybercrime Teaching Guide. Vienna: UNODC.

World Bank. (2020e), The COVID-19 Pandemic: Shocks to Education and Policy Responses. Washington, DC: World Bank.