Journal of Policy Options · RESDO

The Social Consequences of the Information Civilization: Cyber Risks to Youth in the Digital Age

Michael Clark[a]

Abstract

The development of an information society is driving a profound transformation from a material civilization to what can be aptly termed an information civilization. This new era, characterized by the pervasive influence of digital technologies, offers vast opportunities for both society and the economy. Functions such as teleworking, tele-education, and tele-information, all facilitated by the internet, are reshaping social and economic structures. The goal of this study is to highlight the social consequences of the rapid advancement of the information society, with a particular focus on the emerging threats to children and young people in cyberspace. As the digital environment becomes increasingly integral to daily life, it also presents significant risks, especially for the younger population, who are often more vulnerable to online dangers. The research employs a literature-based analysis to examine the phenomenon of cyber threats targeting children and adolescents. This method allows for a comprehensive understanding of the scope and nature of these dangers, with cyberbullying identified as a particularly pressing issue. The study underscores the importance of a broad awareness of cyberbullying, not only among children and young people but also among parents, educators, and policymakers. By bringing attention to these issues, the study aims to foster a greater awareness of the potential risks associated with the information civilization, particularly in relation to the younger generation. It calls for proactive measures to protect children and adolescents in cyberspace, emphasizing the role of education and policy in mitigating these threats. The findings suggest that a concerted effort is required to address the challenges posed by the information society, ensuring that its benefits are maximized while its dangers are effectively managed.

Keywords: Information Society, Cyberbullying, Digital Risks

JEL Codes: I24, L86, D83

1. INTRODUCTION

The emergence of an information society marks a significant transition from material-focused civilization to what can be more accurately termed an "information civilization," where the intangible elements of digital knowledge and communication take precedence. In this new era, the influence of information is pervasive, shaping every aspect of daily life. However, alongside these advancements come profound challenges, particularly in the form of cyberspace-related threats. These threats are especially concerning for vulnerable groups, such as school-aged children and adolescents, who are increasingly exposed to risks in the digital world. The dangers of cyberspace extend far beyond violent behavior found in certain video games. While these types of games may contribute to the normalization of aggression, the threats children and youth face on the internet are much broader in scope. Harmful content, inappropriate interactions with other users, and the accessibility of dangerous online tools all pose serious risks. The anonymity of the internet allows cyberbullying, harassment, and exposure to harmful ideologies to proliferate, often without consequence. This raise concerns not only about immediate harm but also about the long-term psychological and social impacts on young people, who may struggle to navigate these complex and often unregulated environments.

The information and communication revolution has also reshaped the very fabric of society, ushering in a new era where electronic media has become the primary vehicle for work, learning, and communication. The digital age has enabled unprecedented access to information, with online platforms becoming central to education and professional life. Nevertheless, this shift has its downside. While technology offers convenience and connection, it also presents an array of risks, including misinformation, data privacy concerns, and the potential for manipulation. Individuals, especially younger users, may find it difficult to differentiate between credible sources and deceptive content, leaving them vulnerable to exploitation. With the advent of the internet, the world has been introduced to an entirely new digital realm, a space where virtually any type of information can be accessed at the click of a button. The internet has become a dominant force, often replacing traditional media outlets such as radio, television, and print newspapers. Its expansive nature makes it a unique platform for information exchange, but it also makes it a highly unstructured and, at times, chaotic medium. Unlike traditional media, the internet lacks a centralized regulatory framework, resulting in the spread of misinformation, unverified claims, and potentially harmful content. This lack of oversight can create a breeding ground for cybercriminals and malicious actors to exploit

---

[a] International School of Economics, Tbilisi State University, Tbilisi, Georgia

unsuspecting users, including children and teenagers.

Moreover, the internet offers new and immersive experiences that were previously unimaginable. Online gaming, for example, has transformed into a global phenomenon, with thousands of people participating in real-time multiplayer games through mobile devices and gaming networks. These platforms allow users to engage with others across the world, often blurring the lines between virtual and real-world interactions. However, this increased connectivity can have unintended consequences, such as exposure to toxic behavior in gaming communities, addiction to screen time, and even predatory behavior targeting minors. With the internet's ability to foster continuous, non-stop engagement, there is a growing concern about the social, emotional, and cognitive impact this can have on young users. While the rise of the information society has brought many advantages, such as easier access to knowledge, enhanced communication, and the democratization of media, it also presents significant risks, particularly for children and young people. As cyberspace continues to expand, it is crucial for parents, educators, and policymakers to remain vigilant, implementing protective measures that safeguard the well-being of the younger generation. Equally important is the need for digital literacy programs that equip young people with the skills to critically assess online content, identify potential threats, and make informed decisions in an increasingly complex digital world. The global network, often referred to as a "meta-medium," has fundamentally altered the way societies are structured, leading to the emergence of what is known as the "information society." This term is also interchangeably used with "network society," "media society," or the "third wave" in both academic discourse and popular science journalism. Despite the variations in terminology, they all share a core characteristic: communication is primarily conducted indirectly, facilitated by the internet and digital media rather than through face-to-face interaction (Koczy, 2013).

The rise of this information society signifies a profound shift away from the material-based civilization that has historically defined human development. In its place, we are moving towards an intangible, or "invisible," civilization that can more accurately be called an "information civilization." This transformation reflects the growing centrality of digital communication and data in modern life. The functions of an information society are primarily centered around the role of telecommunication and digital networks as multi-functional tools. From the perspective of both economic needs and societal demands, the internet serves a wide range of purposes, including but not limited to teleworking, online education (tele-education), and the provision of information (tele-information). Each of these uses has a ripple effect, influencing various aspects of society in unique ways—whether social, economic, cultural, or even ecological (Castells, 2007). For instance, teleworking allows for increased flexibility in employment, but it also challenges traditional workplace structures and raises questions about work-life balance. Similarly, tele-education broadens access to learning opportunities but may exacerbate inequalities for those without reliable internet access.

As the information society continues to develop, one of its most significant by-products is the increase in anonymity. This heightened anonymity has, in turn, fostered a greater sense of individualism and self-reliance. People are now less dependent on face-to-face interactions and more inclined to pursue personal interests, often within the confines of the virtual world. Social bonds, which were once forged through direct, tangible connections, are increasingly being defined by symbolic exchanges. Online identities, digital representations, and virtual communities now form the basis of many modern relationships, altering the traditional concepts of social interaction and community. The emergence of the information society marks a transformative period in human history, characterized by a shift from material-based to information-driven structures. This evolution has redefined communication, work, education, and even social bonds, placing the internet at the center of modern life. However, as we move further into this information age, it is essential to critically evaluate the social, economic, and cultural implications of these changes, ensuring that they contribute to a more inclusive and equitable global society.

2. DISCUSSION

In most developed countries, a significant portion of the population has established the necessary infrastructure for producing, processing, and transmitting information, as well as for effective communication. Information and communication technologies (ICTs), such as computers and the internet, have become deeply integrated into everyday life, transforming the way societies operate. As more communities become adept at utilizing these technologies, the practical application of ICTs has had a profound influence on national economies. The impact of information technology on national income is particularly noticeable, with the industrial sector and telecommunications services steadily increasing their share in both national income and global production. These sectors are growing more rapidly compared to traditional services and other segments of the economy, reflecting the shifting economic landscape in the digital era. The rise of information technology has also prompted a significant change in social preferences, particularly in the realm of entertainment. Activities such as attending the cinema, theater, or reading books are increasingly being replaced by their digital equivalents. Streaming platforms, e-books, and online media now dominate the entertainment sector, illustrating the cultural shift toward electronic media consumption (Castells, 2007). While this shift offers convenient and accessible options for entertainment, it also underscores the larger societal transformation brought about by the information civilization.

The development of an information-driven society presents numerous opportunities for both individuals and economies. ICTs enable greater efficiency, innovation, and global connectivity, which can fuel economic growth and enhance societal progress. However, alongside these benefits come a variety of challenges, particularly in the realm of cybersecurity. As society becomes more reliant on digital technologies, the risks associated with cyber threats, especially for younger

generations, are escalating. These threats range from data breaches and identity theft to online harassment and exposure to inappropriate content. Addressing these issues is critical in ensuring the safe and secure use of the internet, particularly for children and adolescents. The rapid expansion of internet access has been a defining feature of the modern information society. In 2008, for example, 61% of households with children in Italy had internet access. By 2012, this number had risen to 93%, and by 2016, nearly every household with children (98%) was connected to the global network (Central Statistical Office of Italy, Statistical Research 2012-2016, GUS, Warsaw, 2016). This sharp increase in internet connectivity reflects the growing importance of digital technology in the daily lives of families and children. However, it also highlights the need for greater awareness and education regarding the potential dangers of the digital world, particularly for young users.

The rise of information technology and its integration into both society and the economy has generated significant benefits, fostering innovation, connectivity, and new forms of entertainment. However, these advances are accompanied by new risks, particularly for younger generations who are increasingly exposed to cyber threats. As we continue to embrace the information civilization, it is essential to strike a balance between harnessing the benefits of digital technologies and mitigating the risks they pose. Today's children and youth are growing up in an era where access to the internet is almost universal, shaping their experiences and perceptions from an early age. For this generation, using the internet to search for information, engage with peers, and participate in online communities has become a fundamental aspect of their daily lives. The online world is not merely a tool but an integral part of their social fabric, often occupying a space that feels more natural and immediate than the physical world. This immersion in digital environments has led to a perception of the virtual realm as somewhat detached from reality. Many young people view content shared or downloaded from the internet as inconsequential or purely for entertainment, not recognizing the potential real-world implications (Andrzejewska, 2013).

One of the concerning aspects of this digital immersion is how children and adolescents interpret violence in online spaces, particularly within computer games. For many young players, violent actions depicted in games are seen as normal or even routine, rather than morally wrong or harmful. This disconnection from reality is often reinforced by the absence of immediate physical consequences—players do not experience pain or emotional repercussions while engaging in violent behaviors within the game. As a result, they may not fully grasp the gravity of their actions or the ethical dilemmas posed by such behavior. The virtual nature of these experiences can dull their understanding of real-world violence and its consequences. Research suggests that children who spend significant time playing combat-focused or violent video games tend to exhibit more aggressive behavior in real life. These children are also found to have lower moral standards, as their frequent exposure to simulated violence desensitizes them to the suffering of others and diminishes their sense of empathy and ethical responsibility (Andrzejewska & Bednarek, 2011). The line between the virtual and real worlds becomes blurred, potentially leading to behavioral issues and a reduced capacity for distinguishing right from wrong in everyday situations.

This raises important questions about the long-term impact of virtual environments on the psychological and moral development of young people. While digital platforms provide opportunities for learning, creativity, and social interaction, they also expose children to experiences that can distort their understanding of violence and ethics. It is essential for parents, educators, and policymakers to recognize these challenges and address the potential negative effects of prolonged exposure to virtual violence. By fostering critical thinking, promoting media literacy, and encouraging a balanced relationship with technology, we can help young people navigate the complexities of the digital age without compromising their moral and emotional development. In its early stages, concerns about cybersecurity were primarily focused on violent computer games and malicious messages that circulated online. However, in recent years, the scope of these problems has expanded significantly. Cybersecurity issues now predominantly involve social networking platforms, discussion forums, and cyberbullying, often facilitated through messaging apps or by sharing inappropriate photos taken with smartphones. The digital environment has evolved, and the threats faced by young people have become more diverse and pervasive. Cyberspace presents numerous risks to young users, and these dangers are no longer confined to violent video games. The broader landscape of threats includes malicious behavior from other internet users, as well as harmful content, tools, and platforms that are readily accessible. Whether through social media, gaming communities, or chat applications, young people are exposed to interactions that can lead to emotional, psychological, and even physical harm.

One key concern is the misuse of specific internet applications. The internet, as a diverse and multifaceted medium, offers a variety of platforms, each with its own set of potential risks. Online games, social media sites, instant messaging services, and even platforms dedicated to adult content or gambling can be abused in ways that negatively impact young users. The ease of access to these platforms means that children and adolescents are increasingly vulnerable to their dangers. For instance, excessive use of social media can contribute to issues such as cyberbullying, while online gaming communities may expose users to toxic behaviors and addiction. Furthermore, the rise of online pornography and gambling introduces additional risks related to inappropriate content and compulsive behavior. The growing popularity of specific websites among young users also highlights the importance of monitoring and guiding their online activities. According to an internet survey conducted in Italy, some of the most frequented websites by children aged 7-14 years include platforms like YouTube, Facebook, and popular portals such as Onet, Interia, and NK (formerly Our Class) (Gemius/PBI, 2011). These platforms, while offering entertainment and social interaction, also pose risks if not used responsibly. The influence of these websites on young minds, especially in terms of content consumption and peer interaction, cannot be overlooked. The challenges of cybersecurity have evolved alongside the digital landscape, extending far beyond the realm of violent video games. Today's

online environment exposes young people to a broad range of risks, from cyberbullying and inappropriate content to the misuse of social media and online services. Addressing these concerns requires a comprehensive approach, including better education for young users, stricter regulatory measures, and active parental involvement to ensure a safer online experience. A significant number of Italian teenagers have become regular users of social networking platforms, blogs, and discussion forums. These digital spaces allow them to share their opinions and attract the attention of other internet users. However, the perceived anonymity that the internet offers has contributed to an increase in unethical behavior, particularly among adolescents. One of the most troubling trends in this regard is the frequent use of hate speech, which typically manifests as unprovoked insults, vulgar language, and aggressive comments. This type of toxic communication is especially noticeable in discussions and comment sections on popular platforms like Facebook and other forums. Although hate speech often targets public figures, it can also be directed at ordinary young people, with devastating consequences. The severity of these online attacks can cause significant emotional distress for those affected (Polak, 2014). Research highlights the prevalence of this problem among teenagers. According to a study conducted by the Nobody's Children Foundation, four out of ten young people between the ages of 14 and 17 have encountered hate speech online. Alarmingly, one in five Italian teenagers has fallen victim to hate speech or other forms of online violence. These findings reveal the widespread nature of online aggression, underscoring the urgent need for interventions to protect adolescents from such harmful behaviors. In addition to hate speech, young internet users are also frequently exposed to inappropriate and dangerous content, with pornography being one of the most common risks. A 2016 study conducted by the Orange Foundation, in collaboration with the Children's Health Foundation, examined the online habits of children aged 10 to 18. The results were concerning: 19% of the children surveyed admitted to visiting websites intended for adults. While sites featuring sexual content were the most frequently accessed, children were also exposed to platforms containing vulgar language and violence. Most troubling, the vast majority of these young users (89%) claimed they had entered these websites accidentally. However, exposure to harmful content is more common than it may appear, with 32% of children aged 7 to 18 reporting that they had encountered erotic or pornographic material within the month preceding the survey.

The research also revealed that the likelihood of exposure to inappropriate content increases with age. Among children aged 7 to 12, 27% had encountered erotic or pornographic material, while this figure rose to 33% for those aged 13 to 15. By the time they reached the ages of 16 to 18, nearly half (45%) of the respondents had been exposed to such content (Wójcik, 2016). These statistics highlight the growing vulnerability of adolescents to harmful online material as they progress through their teenage years, raising concerns about the long-term psychological and social effects of such exposure. In conclusion, the internet, while offering vast opportunities for communication and information, has also become a breeding ground for negative behaviors such as hate speech and the consumption of inappropriate content. As the online environment becomes more integral to the lives of young people, the risks they face grow in complexity and severity. Protecting adolescents from these threats requires a concerted effort from parents, educators, and policymakers, along with increased awareness and the development of effective safeguards. It is crucial to ensure that young people are equipped to navigate the digital world responsibly while being shielded from its most harmful aspects.

Sexting refers to the act of sharing or publishing intimate photos via the internet or mobile networks. These messages are often sent as expressions of affection or as "proofs of love" between individuals. However, they carry significant risks, as such images can easily be forwarded, stored, or even used as tools for blackmail or to discredit the person depicted. The dangers associated with sexting were not widely discussed in Italy until recent years. It wasn't until 2014 that the Nobody's Children Foundation conducted one of the first surveys on this issue among Italian youth. The study, which involved adolescents aged 15 to 19 years (CAWI, N = 503), revealed that sexting is a widespread concern. Nearly half of the respondents (45%) reported that they knew friends who engaged in sending intimate messages, while 55% claimed they were not aware of anyone who participated in such activities. Additionally, over one-third of the respondents admitted to having received sexting messages, and approximately one in ten disclosed that they had sent such content themselves (Nobody's Children Foundation, 2014). The rising prevalence of sexting among young people has highlighted the need for greater awareness and education surrounding the risks involved. What may initially seem like a harmless exchange between two people can quickly escalate into a situation where the images are misused, causing lasting emotional and psychological harm. The potential for these images to be shared without consent increases the vulnerability of young people, exposing them to cyberbullying, blackmail, and reputational damage.

Another grave concern in the digital age is the phenomenon of child grooming. Grooming involves the process by which an adult establishes an emotional connection with a child to lower their inhibitions, with the ultimate aim of sexual abuse (Palmer, 2016). Despite the seriousness of this issue, there has been limited research directly addressing the online grooming of children. One of the few comprehensive studies on this subject was conducted in Italy in 2013. The nationwide survey, carried out by the Empowering Children Foundation (formerly known as the Nobody's Children Foundation), focused on violence against children and sampled a representative group of children aged 11 to 17 years (CAPI, N = 1005). The findings indicated that 5.1% of children had received sexual advances or proposals to form acquaintanceships online (Włodarczyk, 2013). These alarming statistics point to the growing risks young people face in the digital world. Online grooming, like sexting, poses a serious threat to children and adolescents, as perpetrators exploit the anonymity and accessibility provided by the internet to prey on vulnerable individuals. Once trust is established, children may be manipulated into sharing personal

information or engaging in inappropriate activities, often without fully understanding the consequences.

Both sexting and online grooming underscore the importance of proactive measures to protect children and teenagers in cyberspace. Parents, educators, and policymakers must work together to foster digital literacy and promote open discussions about the potential dangers of sharing personal content online. Moreover, social media platforms and internet service providers must be held accountable for implementing robust safeguards to prevent the exploitation of minors. Only through collective effort and awareness can we ensure that young people are better equipped to navigate the digital world safely and responsibly. Much of the research conducted on young internet users does not explicitly inquire about experiences of online seduction or grooming. Instead, it tends to focus on cases where individuals meet online acquaintances in real-world settings. This approach reflects the sensitivity of the issue and the often limited sample sizes available for studying such incidents. However, the findings from related studies suggest that the risk of grooming is substantial, with many young people potentially being exposed to this form of online predation. As internet use continues to increase among adolescents, so too does the need for a deeper exploration of grooming behaviors and how to prevent them. One of the challenges in addressing online threats like grooming and cyberbullying is the lack of a clear, legal definition, particularly regarding cyberbullying. Despite its widespread occurrence, neither Italy nor the European Union has established a comprehensive legal definition for cyberbullying, which is broadly understood as a form of violence carried out using information and communication technologies, such as the internet and mobile phones. Some EU member states have made progress by providing official definitions, but a unified approach across Europe is still lacking (European Parliament, 2016). The absence of consistent legal frameworks complicates efforts to combat cyberbullying effectively and leaves many young people without adequate protections.

In the academic realm, efforts have been made to define cyberbullying by identifying its key characteristics. According to British theorist Shaheen Shariff, some of the most precise definitions of cyberbullying come from researchers such as Bill Belsey and Nancy Willard (Shariff, 2008). Belsey describes cyberbullying as the use of information and communication technologies to deliberately engage in repeated, hostile behaviors intended to harm others (Belsey, 2015). This definition emphasizes the intentional and sustained nature of such actions, highlighting that cyberbullying is not a one-time event but rather a pattern of abusive behavior. Willard adds to this by noting that the language used by cyberbullies often includes defamatory remarks, harassment, discrimination, or the disclosure of personal information, and can involve offensive, vulgar, or derogatory comments (Willard, 2003). The call for a legal definition of cyberbullying extends beyond academic circles. The European Union has recognized the need for a common definition of "cyber harassment," which includes elements of cyberbullying but also encompasses other forms of online harassment (European Parliament, 2017). A unified definition would provide clarity and consistency across member states, making it easier to develop laws and policies to protect individuals—especially vulnerable young users—from online abuse. Such legislation would also help to standardize the penalties for cyberbullying and ensure that perpetrators are held accountable for their actions, regardless of where the offense takes place.

The complexities of online threats like cyberbullying and grooming require a concerted effort from researchers, legislators, and policymakers. While academic definitions provide a valuable foundation for understanding the nature of cyberbullying, the lack of a formal legal framework across many regions, including Italy and the European Union, hampers efforts to address these issues comprehensively. Establishing a clear legal definition of cyberbullying and related online offenses is a crucial step toward protecting young internet users from harm. As the digital landscape continues to evolve, so too must the legal and educational measures designed to safeguard children and adolescents in this increasingly connected world. To date, more than half of young internet users in Italy have experienced some form of cyberbullying. The first major public awareness campaign addressing this issue was launched in 2008 by the Nobody's Children Foundation, now known as the Empowering Children Foundation. Despite efforts to combat the problem, cyberbullying remains a prevalent issue within Italian schools, yet its full scale is difficult to measure. The complexity and evolving nature of cyberbullying, which takes many different forms, make it challenging to accurately assess its prevalence and impact.

The basic forms of cyberbullying include a variety of harmful behaviors. Trolling involves deliberately provoking or upsetting others online, while harassment includes persistent, unwanted messages or attacks. Threatening refers to making direct or indirect statements that cause fear, and tracking via the internet refers to stalking someone's online activities. Catfishing, where someone creates a fake identity to deceive others, is also common, as is exclusion, which can involve removing someone from a social media group or network of friends. Although cyberbullying occurs in the virtual world, its effects are deeply felt in the real world, often causing emotional and psychological pain comparable to physical assault. The rapid growth of the internet, combined with the ever-evolving landscape of cyber threats, presents significant legal challenges. Young people are especially vulnerable, and the infiltration of harmful content and behaviors in their online spaces has become a growing concern for parents, educators, and policymakers. However, Italy's current legal framework does not fully address the severity or complexity of cyberbullying. There are many regulatory gaps, and the legislation that does exist is not sufficiently aligned with the seriousness of the issue. As cyberbullying can involve numerous online activities, from defamation to threats, existing laws often fall short of providing adequate protection.

Only the most severe cybercrimes have been incorporated into Italy's Penal and Civil Codes. These include insults (Article 216 of the Penal Code), defamation (Article 212 of the Penal Code), and IT hacking (Articles 267 and 268 of the Penal Code).

Threats (Articles 190 and 191 of the Penal Code) and harassment (Article 190a of the Penal Code) are also punishable, as well as violations of personal rights, which are covered under Articles 23 and 24 of the Civil Code (Pyżalski, 2014). However, many forms of cyberbullying, such as trolling or exclusion, do not fall neatly under these categories, leaving victims with limited legal recourse. The need for stronger legal protections is clear. While existing laws address some of the more overt forms of cybercrime, the nuanced and persistent nature of cyberbullying requires more comprehensive regulation. It is crucial that Italy modernizes its legislative framework to better reflect the realities of today's digital landscape. This would involve not only addressing the gaps in the current legal code but also ensuring that new laws are flexible enough to keep pace with the rapidly changing nature of online interactions. Furthermore, education about the risks and consequences of cyberbullying must be prioritized alongside legal reforms to empower young people to navigate the internet safely.

The issue of cyberbullying in Italy remains a significant problem, affecting more than half of young internet users. Despite public awareness campaigns and some legal protections, the country's legislative framework still falls short of adequately addressing the scale and complexity of the issue. As cyberbullying continues to evolve with the internet, there is an urgent need for Italy to close the regulatory gaps and ensure that children and adolescents are protected from the harm that can occur in the digital world. Research on bullying reveals significant discrepancies in the scale and nature of the problem, largely depending on the type of aggression involved. A major survey conducted in 2010 among secondary school students identified a range of electronic aggression forms. The most common included insults during online chats (experienced by 44% of respondents) and insults during online games (37%). Additionally, unpleasant comments were frequently made on forums (38%) and social networks (28%). These types of aggression are often spontaneous and relatively easy for offenders to commit. In contrast, more deliberate and targeted actions, such as sending unwanted photos (12%), stealing private messages (12%), creating fake profiles (16%), or creating offensive websites (6%), were less common but still troubling (Pyżalski, 2014).

A key issue in addressing cyberbullying is the fact that many young people are not fully aware of the dangers associated with their participation in the online world. They may not recognize that certain behaviors, which seem harmless or part of everyday digital interactions, can actually constitute forms of violence or bullying. Many adolescents believe in the anonymity of the internet, which often leads them to disregard fundamental moral standards. Feeling that their real identities are hidden, they may act in ways they wouldn't dare to in the physical world, engaging in behaviors that cause harm to others. The anonymous nature of the internet can make these actions particularly painful for the victims, as they may feel isolated and attacked even in the supposed safety of their own homes, where harmful messages can still reach them. This sense of anonymity and the ease with which young people can engage in cyberbullying make it an increasingly complex issue to address. Many teens believe that what happens online is inconsequential because they are detached from their real-life identities. However, the consequences of online harassment, slander, and aggression are very real and can have lasting emotional impacts. Young people often underestimate how deeply these behaviors can hurt their peers, leading to long-term psychological consequences for the victims.

Parents and caregivers play a crucial role in safeguarding children from these dangers, but they too face challenges. Many parents place too much trust in their children's ability to navigate the online world independently, believing that as long as their child is at home, they are safe. This overconfidence can lead to a dangerous situation where children are exposed to harmful content or behaviors without adequate supervision or guidance. The internet provides children with unprecedented freedom—freedom to choose what to do, when, and how. Without proper oversight, this autonomy can become overwhelming and expose young people to risks they may not fully understand. For parents and caregivers to build an effective safety system for children online, they need to avoid falling into the trap of over-reliance on trust. Instead, they should become more knowledgeable about the potential risks of the digital world and recognize that a hands-off approach is not sufficient. It is essential for parents to stay informed about the platforms their children use and the dangers associated with them. As Wuszt (2013) wisely points out, electronic media, in and of themselves, are not inherently dangerous. What poses a threat is our ignorance about these technologies and the mistaken belief that children can safely navigate the internet without guidance. The notion that children should be allowed to explore cyberspace entirely on their own is misguided; instead, proactive involvement is key to ensuring their online safety.

While the internet offers a wide array of opportunities for young people, it also presents significant risks, particularly in the form of cyberbullying and online aggression. Addressing these challenges requires a comprehensive approach that involves educating both children and parents about the potential dangers of the digital world. By fostering awareness and actively guiding young internet users, parents can help create a safer online environment where children can explore without fear of harm. Research and interviews with children and adolescents have confirmed the troubling reality of parental ignorance regarding online safety. Despite the significant role parents should play in protecting their children from cyberbullying, many lack the knowledge necessary to create effective safety systems for their children's internet use. This is especially concerning given that most instances of cyberbullying occur while children are at home, with as many as 70% of teenagers receiving insult messages while in the comfort of their own homes (Wołk-Karaczewska, 2012). The home environment, once considered a safe haven, now presents a key battleground in the fight against online harassment. The gap in parental knowledge is stark. Approximately 18% of parents and caregivers admit they lack sufficient knowledge about online safety, while 5% confess to having no understanding of the issue at all. Although 77% of parents engage in conversations with their

children about online safety, these discussions tend to focus on a few common topics: chatting online (57%), encountering dangerous content (51%), and sharing personal information (43%). Despite these efforts, only 53% of parents establish clear guidelines for internet usage with their children, and even when rules are set, they tend to focus narrowly on time limits (57%) rather than more nuanced safety concerns, such as communication with strangers (38%) or the types of websites and services their children can access (36%) (Wójcik, 2016).

Schools also have a critical role to play in addressing cyberbullying. However, teachers and school administrators often share the same lack of awareness as parents when it comes to understanding the scope of the problem. Many educators are either unaware of the prevalence of cyberbullying in their schools or do not realize it exists at all. This lack of awareness leads to the problem being overlooked, and as a result, a trusting relationship between students and teachers is often absent. Victims of cyberbullying may not feel comfortable confiding in teachers, and educators often only become aware of the problem once an incident has occurred. The failure to prevent or respond effectively to cyberbullying exacerbates the issue, leaving both students and teachers ill-prepared to deal with its impact. Moreover, the lack of knowledge about cyberbullying prevention is further compounded by the absence of a coordinated response to this issue in many schools. Cyberbullying is rarely addressed in school curricula, and discussions about the topic with students are infrequent. This lack of focus on digital safety in educational settings leaves students vulnerable to online aggression and unprepared to navigate the complexities of the digital world. Schools must begin incorporating cyberbullying awareness and prevention strategies into their curricula to address this growing threat. The phenomenon of cyberbullying is one of the most significant dangers facing today's youth, and it requires immediate attention. Given the complexity and potential severity of cyberbullying, there is an urgent need for schools to implement both preventive and intervention measures. This includes not only raising awareness but also developing tailored solutions that reflect the unique needs and circumstances of each school environment (Grądzki, 2013). Pupils need to be taught how to use digital media responsibly so that these tools do not become vehicles for aggression or peer violence. Furthermore, children must be made aware of the possible consequences of risky online behavior, so they can better protect themselves from harm.

The combined ignorance of parents and educators about cyberbullying represents a significant barrier to effectively addressing this issue. Both groups must become more informed and proactive in safeguarding children from the dangers of the digital world. Schools should integrate digital literacy and online safety into their curricula, while parents must take a more active role in guiding their children's internet usage. Only through collective efforts from both the home and school environments can we begin to combat the pervasive issue of cyberbullying and ensure that children have the knowledge and tools to navigate the internet safely.

3. CONCLUSIONS

Cyberspace presents numerous dangers, particularly for children and adolescents, and these threats have evolved and expanded rapidly in recent years. While research to date has primarily focused on identifying the frequency and forms of these dangers, there is a growing consensus that this research needs to be broadened. Expanding the scope of research would allow for the development of more effective and systemic prevention strategies to combat these risks. Currently, much of the research relies on questionnaires, which, while useful, often produce large discrepancies and inaccuracies in assessing the true scale and diversity of the problem. Despite these challenges, there is no question that the prevalence of online threats is alarmingly high, and the consequences for young users are deeply concerning. Among the various types of harmful content that children and young people encounter online, pornography remains the most common. However, other dangers—such as sexting, online grooming, and cyberbullying—are equally harmful and can have long-lasting effects on the psychological and emotional well-being of young people. The ease with which children can access inappropriate material, coupled with the anonymous nature of online interactions, exacerbates these risks, making it essential to implement robust prevention and intervention measures. Given the magnitude of the problem and the slow response from many institutions to implement systemic prevention measures, there is an urgent need for national legislation to spur the introduction of effective actions against cyber threats. Policymakers must prioritize the development of legal frameworks that not only punish offenders but also prevent young people from becoming victims of online exploitation and abuse. Such legislation would provide the foundation for a coordinated response to the challenges posed by cyberspace, including better regulation of harmful content and stronger protections for children and adolescents. One of the most significant challenges in addressing these cyber threats is reaching parents effectively. Parents are a critical part of the solution, but they are often difficult to engage. Many schools still fail to provide parents with sufficient information about online safety, and even when information is shared, there is often a poor response from parents. Unfortunately, many parents tend to shift the responsibility of educating their children about online risks to schools, thus diminishing their role in ensuring their child's safety in the digital world. This transfer of responsibility creates a gap in the protective measures that should be in place at home. To address this issue, it is imperative to launch a comprehensive and engaging campaign aimed at encouraging parents to take an active role in safeguarding their children online. Such a campaign should be designed to raise awareness of the specific dangers present in cyberspace and equip parents with the tools and knowledge they need to protect their children. Importantly, the campaign should also highlight the shared responsibility between schools and parents in creating a safe online environment for young users. By fostering collaboration between these two key groups, the campaign would help close the gap in online safety education and

ensure that children are protected from the growing dangers of the internet. In conclusion, cyberspace is filled with significant dangers for young people, and the rapid development of these threats requires a concerted and systemic response. Expanding research efforts to better understand the scope of the problem, along with national legislation and parental involvement, is essential in combating cyber threats. A coordinated approach that includes schools, parents, and policymakers is crucial to creating a safer online environment for children and adolescents. By taking immediate action, we can mitigate the risks posed by cyberspace and ensure that the internet remains a safe and enriching space for young users.

REFERENCES

Andrzejewska, A. (2013). *Children and Youth Communication in Virtual Space*. In: A. Andrzejewska, J. Bednarek, S. Ćmiel (Eds.), *Man in the Real and Virtual World*. WSGE, Józefów.

Andrzejewska, A., & Bednarek J. (2011). *Cybercrime Risks Education and Health Aspects*, Training Materials for Teachers and Educators. Warsaw.

Belsey, B. (2015). *Cyberbullying: An emerging threat to the 'always on' generation*. Accessed 24 October 2017.

Castells, M. (2007). *Age of information: economics, society and culture. Volume 1, Network Society*. Scientific Publishing House, Warsaw.

Ćmiel, S. (2013). Protection of minors in cyberspace through a secure on-line environment in the European Union's activities. In: A. Andrzejewska, J. Bednarek, S. Ćmiel (Eds.), *Man in the Real and Virtual World*. WSGE, Józefów.

Czesławiak, A. (2007). *Bullying and cyberbullying as new forms of threat to pupil's safety*. Siedlce.

European Parliament. (2016). *Study: Cyberbullying among young people*. Directorate General for Internal Policies, PE 571.367.

European Parliament. (2017). *European Parliament resolution of 3 October 2017 on the fight against cybercrime* (2017/2068(INI), P8_TA (2017)0366).

Gemius/PBI. (2011). *12% of Polish Internet users are children. What websites they choose?* Accessed 24 October 2017.

Nobody's Children Foundation. (2014). *FDN - Sexting among Polish youth: Results of the quantitative study*. Warsaw.

Polak, Z. (2014). Harmful content. In: A. Wrzesień (Ed.), *Online safety of children: A compendium for parents and professionals*. Warsaw: Nobody's Children Foundation.

Razza, K. (2015). Cyber-bullying: an analysis of the European framework on cyber-bullying. *Sweet and Maxwell - Computer and Telecommunications Law Review, 21*(7), 193-203.

Shariff, S. (2008). *Cyber-Bullying: Issues and Solutions for the School, the Classroom and the Home*. London: Routledge.

Wójcik, Sz. (2016). *Internet threats to children and young people*. TNS, Orange Poland, Orange Foundation.

Wójcik, Sz. (2017). *Children count in 2017*. In: *Child Abused: Theory of Practice Research, 16*(1). Warsaw.

Wołk-Karaczewska, A. (2012). *Cyberbullying at school*. Colourful Media, Poznań.