Research has proven that there are countless benefits for children in the digital world, but this has simultaneously highlighted their vulnerability through exposure to harmful and unethical programs and abuse, which is expected to increase beyond the coronavirus pandemic restrictions, and into the fourth industrial revolution.

This policy brief recommends the United Nations to adopt a global protection approach to the digital world of the child, by adding an optional protocol to The Convention on the Rights of the Child, through a global interdisciplinary effort. We suggest a framework of five main elements: Principles, Prohibition and criminalizing acts, Prevention, Protection, and Pursuit of all elements.

Challenge

Children are active online from an early age. Globally, one in three internet users is younger than 18 years (Macenaite and Kosta 2017). Despite the countless positive effects of digital media on children, they remain vulnerable to harm through exposure to unethical information and behaviors, emphasizing the need to govern new waves of digital innovation. Sustainable and inclusive growth entails not only opportunities, but also high risks for our children (Communiqué 2019).

The challenges include:

• **Implementation of child protections**
  Although the Convention on the Rights of the Child (CRC) in its articles recognizes the rights of children to protection and participation, children remain vulnerable to harm through media, video games, and online contacts. Further, the gap between intention and action continues to grow (Macenaite and Kosta 2017; Buckingham 2000).

• **Growing rate of victims among children using the internet and video games**
  Statistics indicate that increasing numbers of children suffering from gaming disorders, cyberbullying, sexual abuse, online gambling, obesity, privacy risks, damage to reputation, and discrimination online (Macenaite and Kosta 2017; King et al. 2018). The UNESCO report on Ending School Violence stated that at least 10% of children are affected by cyberbullying (UNESCO 2019), with estimates varying between 10% and 40%, depending on the definitions and the age group (Cyberbullying Research Center 2019). Adolescent victimization rates have doubled in the USA between 2007 and 2015 (Miller 2017). Studies show that children exposed to violent video games are more likely to commit acts of violence and exhibit moral disengagement in real life situations. Furthermore, they are more vulnerable to criminal acts (Teng et al. 2019).

• **Effects of the coronavirus pandemic**
Although the interpretation of the changes in quantitative data is premature, current research on the impact of the coronavirus pandemic restrictions on child cyber abuse indicates the following alarming trends: increased screen time during the pandemic, decreased adult supervision, increased emotional vulnerability due to restrictions, higher probability of offenders acting on impulse due to travel restrictions, economic hardship, and governments shifting their focus away from child abuse to implement coronavirus pandemic controls. Web-IQ has revealed that from February to end-March 2020, posts on known child sexual abuse forums increased by over 200%. The India Child Protection Fund (ICPF) has registered a spike in online searches for child sexual abuse since the beginning of lockdown in India. Similarly, the UK National Crime Agency’s analysis of online chats indicates that offenders are discussing new opportunities to exploit children during lockdown (We Protect Global Alliance 2020).

- **Generational gap in technology and digital media use**
In a rapidly growing and transforming digital environment, young people rapidly master new technologies, exacerbating the generation gap in the production of effective protection systems. Parents and caregivers can actively engage with technology by obtaining digital knowledge and balanced digital habits (Blum-Ross and Livingstone 2016). Any approach to bridging the generational gap to protect the child should consider the differences in the media proficiency of parents, which is influenced by socio-economic status, educational background, and family structure (Nikken and Opree 2018).

**Proposal**

Electronic media has many positive effects on children, contributing to their education, creativity, entertainment, self-fulfilment, health, safety, and civic and political participation (Buckingham 2000; Third and Lemm 2019; Third et al. 2017). However, children are exposed to harmful electronic games and sexual and emotional assaults. In Saudi Arabia, 59% of young people believe the internet should be more tightly regulated (Dennis, Wood, and Saeed 2017). Cyberbullying through digital media deeply affects the psychological growth and mental wellbeing of children and can—as an extreme—result in antisocial behavior or suicide (Felt 2015; El Asam and Samara 2016). General discussions held in Geneva in September 2014 recognized the reciprocal nature of online and offline actions and consequences (Third and Lemm 2019). Furthermore, digital media practices potentially lead to mental health and physical issues such as obesity, poor eyesight, and anxiety (Third and Lemm 2019).

In May 2019, the World Health Organization (WHO) officially classified gaming disorder as an illness in the International Classification of Diseases 11th Revision (ICD-11). The American Psychological Association (APA) has decided to follow the WHO classification and will officially recognize gaming disorder in the DSM-5 (Gansner 2018).

**Main recommendation: Collaboration of the United Nations and the Convention on the Rights of the Child**

Our main recommendation is that G20 governments and international organizations collaborate with the United Nations (UN) in reforming the Convention on the Rights of the Child (CRC) by producing a new additional Protocol to it, which could be named “Optional Protocol to the Convention on the Rights of the Child on Protecting Children on the Digital World”. G20 governments and international organizations should collaborate with the United Nations (UN) in reforming the CRC by formulating the “Optional Protocol to the CRC for the Protection of Children in the Digital World”. This new protocol must govern all forms of digital child abuse, aligning and strengthening articles 4, 13, 17, 19, 24, 31, 32, 34, 36, and 39 of the CRC, and reforming those articles referring to the digital age (UN Convention on the Rights of the Child 1989). This will address the shortcomings in child protection by introducing guidelines and regulations to all nations and existing entities, promoting the development of their own child protection policies to strengthen the implementation of the CRC, and play an important role in governing and monitoring stakeholders (producers, society, and users such as children, family and teachers). Additionally, the limits of freedom and associated risks online for both children and adults should be understood, regulated, and governed, while preserving the undisputed benefits.

**Global collaboration and interdisciplinary work**

Given all the risks, there have been increasing calls for interdisciplinary work to protect the child in digital media. Policy makers, academics, technologists, psychologists, educators, journalists, media, and production agencies should work together in a holistic manner to safeguard children’s digital virtual world (Schneier 2019), by delivering a global prevention and protection system through global collaboration under the supervision of the UN to strengthen the CRC and its application.

**G20 countries are key players**
The current complexity of digital media requires innovative and interactive strategies to enable child protection across the world. The G20 countries are key players in setting and delivering a global protection system, and in reforming existing international regulations and policies to tackle new global problems of child protection and participation in digital media as digital crimes travel across borders. The influential countries of the G20 have control over resources (fund, data, and research) and own global search engines that could lead international collaboration towards efficient global governance of child rights in the digital world.

**Organizational support**

We anticipate an international, sustainable, and committable long term policy supported by the UN, the Organization for Economic Cooperation and Development (OECD), the World Bank Group (WBG), the World Health Organization (WHO), and the World Trade Organization (WTO) as these respected organizations are key players in reforming the CRC and are present in G20 meetings; they should, therefore, be involved in cooperating in protecting children by collaborating in the production of the new protocol, thereby fulfilling the United Nations Sustainable Development Goals (SDGs).

In revision of the G20 policy briefs: Certain policies discuss a general transformation of the digital age and artificial intelligence (AI) and its implications mostly on the adult world, or policies developing the benefits of internet use in education in general, for example in Kiriya (2019). However, there are no policies discussing the harms of technology and the digital world on the child. This policy brief finds that safeguarding children in the digital environment is as important as safeguarding their physical environments from the detrimental effects of climate change, emissions and food security – key issues for the G20. Thus, this policy brief concentrates on the negative aspects of the digital world to govern the harm it poses to children. This approach also allies with the Saudi approach of steering the G20’s work for a physically and mentally healthy, and educated youth.

**Framework for the proposed protocol**

Purpose: This protocol should govern all forms of digital child abuse, allying, strengthening, and reforming CRC articles (UN Convention on the Rights of the Child 1989) for the digital age.

Digital abuse is a new form of child abuse. The WHO’s definition of ‘Child abuse’ or ‘maltreatment’ constitutes all forms of physical and/or emotional ill-treatment, sexual abuse, neglect or negligent treatment, and commercial or other exploitation resulting in actual or potential harm to the health, survival, development, or dignity of the child within a relationship of responsibility, trust, or power (WHO 1999). The British Council added bullying as a form of abuse defined according to its severity, highlighting that children can also be perpetrators of abuse. The British Council applies E-Safety to internet technologies and electronic communications via mobile phones, games consoles, and wireless technologies (Child Protection Policy 2018).

Suggested five elements (The 5Ps):

1. **Principles:**
   This policy brief suggests the following principles—some of which are CRC principles—underlying the articles to protect the child virtually:
   
   - Best interests of the child are paramount and shall be the primary consideration in decision-making.
   - Respect for children’s rights, including the right to protection, safe entertainment, participation, access to information, and privacy.
   - Child and adult rights-to-freedom in harmful situations are to be anticipated.
   - Equality of opportunity to ensure that all children have the same rights to protection.
   - Cultural sensitivity, respect for religious and ethical values, and recognition of local contexts in decision-making. Local laws, regulations, and procedures are always respected.
   - Guarding confidentiality of sensitive personal data. Information can only be accessed, shared, and processed on a strict need-to-know basis solely for the purpose of conducting official duties.
   - Working with others to protect children, both nationally and internationally with different organizations, including law enforcement and specialist child welfare agencies where necessary.
   - Interdisciplinary approach to combating child digital abuse in a holistic manner by policymakers, technologists, educators,
psychologists, journalists and media, and agencies.

- Integration of online and offline dimensions: acknowledging that children engage with digital media online and offline (Third and Lemm 2019).
- Organizations and individuals developing, deploying or operating child material should be held accountable for their proper functioning in line with all the above principles.
- Monitoring the implementation of the Child Protection Policy (2018) internally and through regular reporting to the UN in line with the CRC.

2. Prohibition

- The global and national identification, classification and criminalization of harmful acts against children in the digital world (including child sexual abuse, grooming, child exploitation, producing, distributing, offering, using or selling harmful—both mentally and physically—digital or communication material), as well as defining penalties and procedures to be enforced.
- The need for an industry-wide global code-of-conduct to protect children from being in contact with any harmful content, including pictures, adverts, and games, among others.
- Rules and regulations to regulate organizations, agencies, partners, contractors, and suppliers that provide goods, services, apps, programs, and games for children.
- Universal, mandatory applicability of a zero-tolerance approach. All necessary efforts must be made to comply with the policy irrespective of cost implications or operational inconveniences incurred.
- Criminalizing the unnecessary collection, use, or spread of the personal information of a child, by any website operator or online service provider that violates the regulations described under this protocol.

3. Prevention

- Reducing consumer demand for products that are harmful to children by spreading public awareness. Directed programs must be deployed through conventional and new media channels.
- Promoting online educative opportunities that provide healthy alternatives in supporting the rights of the children to safe education and entertainment.
- Educating children, parents, teachers, technologists, law firms, and parliaments on the dangers online facing children; laws and education programs should focus on the prevention and response to these risks through a “training for all” approach.
- Providing training and support to agency workers, producers and developers to recognize and eliminate harmful material in applications and games targeting children.
- Education and training of local police, INTERPOL, and specialized local and global organizations that prevent and respond to child protection risks and incidents.

4. Protection

- Creating global partnerships for the protection of the child, including research, awareness programs, technological assistance, law enforcement, follow-up of cases, and the arrest of criminals.
- Defining what constitutes the personal information (data) of a child (for example, first and last name, home address, phone number, user name, photos and videos, geo-location, and parents’ information, among others), aimed at protecting the child.
- Identifying different national and global entities that are responsible for child protection, case follow-up, and action-taking.
- Defining procedures to facilitate action in support of children at risk or in harmful situations.
- Encouraging and funding NGOs and special centers to create a safer internet platform for children.
- Selecting an empowered entity in every country as a reporting channel for information and advice.
- Defining and clarifying reporting steps for all stakeholders (including children, parents, and teachers, among others).

- Focusing on the most vulnerable children, such as those in refugee camps, street children, children with special needs, and girls, as they tend to be more active users of digital media and in some cultures tend to develop relationships through it (Third and Lemm 2019).

5. Pursuit

- Emphasizing accountability and responsibility in fulfilling duties and obligations to protect children.

- Providing flexibility to safeguard all future internet activities considering the fast pace of its development, the slow implementation of laws (according to an EU–BIK study), and that children are quick learners in this field.

- Encouraging and funding evidence-based research at all levels regarding online child abuse and social media communication, to be shared and used according to national and international need.

- Entities responsible for child digital protection submitting regular reports locally to respective governments, and/or national human rights organizations.

- Each country that has signed this protocol is to submit special reports to the UN, which include all information, progress, and actions taken within a specific time.

- Systematically reviewing existing legislation in this protocol as applied to digital media practices affecting children (Third and Lemm 2019).

It is recognized that at the country level, authorities would have to identify ways to fulfill the requirements of the protocol by considering the inclusion of any criminal jurisdiction in accordance with local laws given their local operating conditions and legal provisions.

Examples of government initiatives

In conclusion, there are a few examples of systems available in certain countries. This is far from a complete work but reinforces the need for the additional protocol to benefit children.

In Saudi Arabia, the Electronic Crime Act (2007), and Child Protection Act (2014) have useful objectives to protect users, ethics, and public interest, and have had a positive effect on minimizing child abuse rates. However, they need to be developed to cover all digital aspects of abuse to protect children’s psychological growth and health. Other countries are lacking such laws.

The government of South Korea has developed a coordinated system of eight ministries and several other entities to combat gaming disorder and provide a healthy online environment for children. Chinese laws have sought to restrict and censor internet gaming activities. From 2000 to 2014 foreign gaming consoles were banned from commercial sale in China. The Ministry of Culture (MoC) was responsible for the implementation of the online gaming Anti-Addiction System, whereby children under 18 years of age are restricted to three hours play per day with longer hours resulting in deactivation or compromised in-game reward mechanisms. Under these regulations, any internet gaming or online products are prohibited from including gambling, pornography, violence, or any content considered to violate the law. Underage players are forbidden from purchasing virtual currency in internet games.

The USA, the UK, Australia, Germany, Japan, and Taiwan have promising prevention approaches comprising school-based programs for healthier internet use in adolescents, but their efficacy warrants further empirical attention (King et al. 2018; Lee et al. 2013). These countries have recognized excessive screen time as a health hazard. The UK National Institute for Health and Care Excellence (NICE) has guidelines for reducing obesity and acknowledges the importance of limiting computer and video game playing time. Guidelines and policy recommendations for addressing Internet use are increasingly being produced, including the American Academy of Pediatrics (2011) position statement on screen time in younger children, which includes recommendations for the USA to adopt a prevention model comparable to those in East Asia, including implementing mandatory media education in school curricula (King et al. 2018). In Japan, video games are generally regulated by self-imposed controls and voluntary ratings by third parties, rather than by law (Yuichiro 2018).

The Better Internet for Kids Policy Map (BIK) strategy in the European Union (EU) was created to compare and exchange knowledge on policymaking and implementation in EU Member States on the themes and recommendations of the European Strategy for a Better Internet for Children. The BIK map comprises five fields. They are stimulating quality content online for young people, digital/media literacy in
education, stepping up awareness and empowerment, tools and regulation for an online safe environment, and legislation and law enforcement against child abuse. Member states of the EU report wide support for policy provision, but many gaps remain both in terms of policy governance and stakeholder participation (O’Neill and Dinh 2018).

Disclaimer
This policy brief was developed and written by the authors and has undergone a peer review process. The views and opinions expressed in this policy brief are those of the authors and do not necessarily reflect the official policy or position of the authors’ organizations or the T20 Secretariat.

References


Existing Initiatives & Analysis