T20
SAUDI ARABIA 2020
THINK

POLICY BRIEF

FOSTERING A SAFER CYBERSPACE FOR CHILDREN

Task Force 6

ECONOMY, EMPLOYMENT, AND EDUCATION IN THE DIGITAL AGE

Authors

MUHAMMAD KHURRAM KHAN, OMAIMAH BAMASAG, ABDULLAH AYED ALGARNI, MOHAMMAD ALQARNI

موجز السياسة

تعزيز فضاء إلكتروني أكثر أمانًا للأطفال

فريق العمل السادس

الاقتصاد والتوظيف والتعليم في العصر الرقمي

المؤلفون

محمد خرام خان، أميمة باماساج، عبد الله عايد القرني، محمد القرني

ABSTRACT

Our world is more connected than ever before. Among the billions of people online, children are increasingly using the internet for their learning and growth in significant ways. This hyper-connectivity exposes children to a multitude of risks, which is becoming a global phenomenon. Policymakers must map out urgent strategies and plans to tackle the challenges in protecting and safeguarding children connected online. Therefore, it is imperative to establish global capacity building programs, launch collaborative and multi-stakeholder initiatives, strategize transnational legislation, and develop frameworks and programs for the well-being of children online.

لقد أصبح عالمنا أكثر تواصلاً من ذي قبل. ومن بين مليارات المستخدمين على الإنترنت، يتزايد استخدام الأطفال الإنترنت في تعليمهم ونموّهم بطرقٍ فعَّالة. ويعرض هذا التواصل المفرط الأطفال إلى مخاطر جمَّة، وهو ما أصبح ظاهرة عالمية. ولا بد أن يضع صُنّاع القرار استراتيجيات وخططًا عاجلة من أجل معالجة تحديات الحماية والسلامة للأطفال المتصلين بالإنترنت. وبناءً عليه، أصبح من الضروري تأسيس برامج عالمية لبناء القدرات، وإطلاق مبادرات تعاونية متعددة أصحاب المصلحة، وإجراء تخطيط استراتيجي للتشريعات الانتقالية، ووضع أطر عمل وبرامج لرفاهية الأطفال المتصلين بالإنترنت.

CHALLENGE

Children represent over 25% of the world's population and being online is an important part of their lives. It is estimated that approximately one billion children were using the internet in 2018 (UNICEF 2018). However, due to the coronavirus pandemic and with the introduction of strict social distancing and quarantine measures, there is a global surge in the number of children and young people using the internet, mobile apps, and digital technologies. Amid the pandemic, more than 1.5 billion children and young people have been affected by school closures worldwide, which ultimately heightened internet usage due to online education (UNICEF 2020). Stringent precautionary procedures implemented by many countries to slow the spread of virus, such as lockdown measures or stay-at-home policies, have led children to socialize online. This includes spending more time on social media and online gaming networks.

This increased use of the internet also heightens the risk of children being exposed to inappropriate content such as photos, videos, and applications, which can be employed to harm them in many ways. Furthermore, their risk of being connected to strangers and online predators is increased. Psychological motives, such as the desire for entertainment or making new friends, encourage children to talk to strangers over the Internet (Peter et al. 2006; Vandoninck et al. 2011).

The potential online risks for children can be classified into three main areas as the three Cs (Raising Children Network 2018).

1. Content risks

These risks include things that may cause school-aged children to feel discomfort or disgust when accidentally encountering them online. This might include violence, pornography, and images of cruelty to animals.

2. Contact risks

These risks include children making contact online with strangers or adults masquerading as children. For example, a child might be lured to meet a stranger or enticed to share personal information.

3. Conduct risks

These risks include children behaving in ways that might hurt others or result in them becoming victims of inappropriate behavior. This could include a hateful blog or post or uploading material online which could incite racism and offend other readers.

The WeProtect Global Alliance (2020) published an intelligence brief in April 2020, which included predicted threats to children during the period of COVID-19 restrictions. Some threats in their report include: increased online child sexual exploitation; greater unsupervised internet use and therefore greater risk of sexual coercion, extortion, and manipulation by offenders; greater numbers of emotionally vulnerable children and therefore, increased risk of grooming by offenders; lack of prioritization by governments and law enforcement agencies on combatting online child sexual exploitation in many jurisdictions due to their current focus on COVID-19; and increases in livestreaming of abusive in-home environments due to economic hardships and the inability of offenders to travel.

The Group of Twenty (G20) community recently proposed policy briefs that tackle cybersecurity awareness from various perspectives. Carin (2017) discussed the challenges of ensuring a secure, robust, sustainable, and accountable digital economy with focus on the financial sector. One recommendation is to educate the public on cyber-hygiene. A policy brief by Schwarzer et al. (2019) addressed cybersecurity as one of the main challenges to the success and health of both government and the private sector endeavors, including defining appropriate levels of cybersecurity regulation for each sector. A recommendation of the policy brief in Business20 (2017) is for the G20 community to cooperate and improve cybersecurity by providing a secure infrastructure for the digitized economy to succeed.

These policy briefs address the cybersecurity and awareness issues from a general perspective. There is a lack of policy work proposed to the G20 that focuses specifically on the online safety of children.

PROPOSAL

Any meaningful improvement to the safety and protection of children online, must come from the highest authority. Therefore, we believe that the G20 has a crucial role to play in leading the efforts to create a safer cyberspace for children. The following recommendations aim at providing implementable initiatives that can assist G20 member states achieve this goal.

Proposal I

Establish a center of excellence for the online safety and protection of children

Protecting children online is a global issue; therefore, global response and cooperation is needed to address it. There are many initiatives by different international organizations, including the International Telecommunications Union and UNESCO, dedicated to the online protection and safety of children, but these are insufficient in a hyperconnected world where children interact online through web browsing, education, social media, gaming, and entertainment websites and applications. The COVID-19 era has escalated the demand for the protection of children online, which exceeds the scope and capacity of UNESCO or the International Telecommunication Union (ITU) and requires greater coordination and synergy between international organizations and governments.

Therefore, it is highly recommended that the G20 establish a center of excellence for the protection and safety of children online. This center should function as a central point of contact and source of coordination for building capacity and capability at the global, regional, and national levels. It should work in collaboration with multi-stakeholders, including international bodies, governments, law enforcement agencies, academic experts, policy makers, religious figures, and civil society to promote awareness strategies and legislative measures at strategic, tactical, and operational levels to address the safety of children online. It is suggested that the G20 establish this center in Saudi Arabia, which recently launched a global initiative for child online protection (National Cyber Security Authority 2020).

Proposal II

Develop a framework to protect children from online radicalization and extremism

Radicalization and extremism are global security threats that significantly impact the well-being and stability of our society. Terrorist organizations have penetrated cyberspace and exploit it in different malicious ways, from online recruitment and fundraising to the broadcasting of violent content. Children are unfortunately becoming soft targets for such threats (Morris 2016). The most commonly used medium by cyber perpetrators to promote and engage in violent and extreme ideologies are social

media platforms and gaming applications, which is fueling the rise of right-wing extremism, while violence and intolerance threaten children as both actors and targets simultaneously.

Combatting extremism should be considered as a global shared effort and the G20 should establish a more robust framework of best practices to identify, prevent, and eradicate this menace from society. It should further promote equality, prevent marginalization, strengthen children's resilience to dark forums, and fortify cooperation between online communities and law enforcement authorities to report, investigate, and eradicate outlets targeting children online. Finally, protecting children from the risks of online radicalization, extremism, and terrorism should be incorporated as an integral part of school curricula to build their awareness of these dangers while surfing the internet.

Proposal III

Establish a strategy for a safe online environment

Several reports argue that internet governance bodies should protect the rights of children online (Livingstone, Carr, and Byrne 2016). The G20 should develop a strategy to ensure that the rights of children online are protected. This strategy should be guided by and allied with the existing international normative framework for children's rights, as well as decisions and policies agreed upon in the United Nations intergovernmental bodies such as UNICEF. The strategy should include two main goals: 1) to promote a safer cyberspace for children, and 2) to empower them to protect themselves from online risks.

The United Nations Educational, Scientific, and Cultural Organization (UNESCO); the Council of Europe; the Organization for Economic Co-operation and Development (OECD); and the NETmundial initiative converge around human rights and protection from illegal activity (Phippen 2017). However, more efforts are needed to safeguard children online (Burns and Gottschalk 2019, Livingstone et al. 2017). Multi-stakeholder initiatives should be launched by the G20 in coordination and cooperation with these international organizations and educational institutions to empower children to protect themselves from online threats. Stakeholders should include governments, companies, civil society, internet service providers, and other entities involved in maintaining a safe cyberspace. Collaborative initiatives should be established with the specific aim to advance security literacy, training, re-skilling, and upskilling children to adequately protect themselves. This includes creating awareness for children in schools, providing updated information about risks, and sharing best practices. The importance and urgency to launch this initiative has grown recently and will continue to grow in the post-COVID-19 world.

Proposal IV

Incentivize public and private sector organizations

Public and private sector organizations are generally mandated by law, incentivized, or self-motivated to adopt institutional policies that enhance the safety of children (OECD Council 2012). Similarly, the G20 should incentivize public and private sector organizations, such as IT companies, small businesses, start-ups, and research parks through tax incentives, loan programs, rebates, grants, or other public policies to develop and implement cybersecurity skills training to assist educators in empowering and upskilling children. However, incentivizing public and private sector organizations requires having a performance evaluation entity, which should offer policymakers a reliable means to measure achievements and failures. It is also necessary to evaluate levels of compliance, the achievement of objectives, and the need for adjustments. The OECD Council (2012) suggested that including independent evaluations would increase compliance monitoring and enhance policy effectiveness. It would also improve transparency and accountability of private and public stakeholders. The G20 should further adopt the same performance evaluation model to track the key performance indicators of participating organizations under this initiative.

Proposal V

Create a multi-stakeholder policy framework

The challenges of children's online safety and protection require a multi-stakeholder approach (Burns and Gottschalk 2019). Industry, law enforcement, non-governmental organizations (NGOs), and government must work together. Fortunately, there are many examples of such participation and cooperation. UNICEF has used its success and experience in fostering partnerships to build innovative strategies for 'shared value creation' with the WeProtect project (Children's Rights and the Internet 2016). The Safer Internet project in the EU is another example of a multi-stakeholder framework that involves and collaborates with the public sector, technology and media industry, and civil societies (mainly NGOs). Therefore, a goal of the G20 should be to foster multi-stakeholder participation and cooperation to anticipate and interpret trends, keep ahead of the technology curve, spread awareness of these new challenges, and highlight to policymakers and the public the importance of the safety and protection of children online. The G20 should play an instrumental role in helping children in vulnerable nations who could become more susceptible to online risks due to limited digital literacy and resources.

Proposal VI
Develop a multilingual children's online protection guide

Not speaking English has been a barrier in child protection, not only online but in general (Chand 2005). While the use of interpreters is a solution in the real world, it is not feasible in cyberspace. This has prompted the EU to provide content in its members' native languages to guarantee that such contents are accessible to all regardless of their social status (which usually reflects their language capabilities). This is crucial as connectivity is common to all classes of children. However, aside from the EU effort, there is little coordinated effort elsewhere. Individual countries develop their own children's online protection guides in their local languages. The government of Singapore provides their guide with content in English, Mandarin, Malay, and Tamil (Cyber Security Awareness 2019). While this is a positive start, we believe that more coordinated multilingual efforts would result in better-quality guidelines. Therefore, G20 member states should work together to develop a multilingual online protection guide for children that benefits from the experiences and expertise of all its members. This will guarantee that an underdeveloped community would have the same access to information guidelines as the developed community.

Proposal VII
Build international norms and standards for child online safety

The Child Online Safety Index (COSI) is a real-time indicator that assists countries in understanding their position regarding children's online safety (DQ Institute 2020). The COSI assesses the online safety status of children worldwide using six metrics: cyber risks, disciplined digital use, digital competency, guidance and education, social infrastructure, and connectivity. For each country, COSI calculates a score ranging from 0 (minimum online safety for children) to 100 (maximum online safety for children). This provides the corresponding countries with guidance in identifying which areas of child safety online require more attention. The G20 member states should consider and acknowledge this index as a global standard.

Within educational contexts, the G20 community should work together to establish a framework of cyber standards and procedures to maintain the online safety of scholars. These should include the establishment of procedures to ensure that students are fully informed on appropriate and safe online procedures, including installing and using spam- and ad-blocking and filtering tools on school computers to control access to harmful content. An example of such standards is an Acceptable Use Policy (AUP), which is a written agreement between students, parents, and school repre-

sentatives that lists the terms of safe Internet use and the consequences of misuse (REMS 2020). Parents are normally expected to confirm that their children will adhere to these guidelines, and students accept the terms explained in the policy. AUPs can include topics such as expected online behavior, accessible online websites, academic ethics while using technology, and data protection policies.

Proposal VIII

Enhance the safety of children online by strategizing transnational legislation

During these unprecedented times of COVID-19, it is important for our children to master the basic technical skills to use digital devices and resources for online educational purposes. However, it is equally important to ensure that they are safe and responsible cyber citizens. Law enforcement related to cybercrimes targeting children is crucial to ensure cyber safety and protect them from these threats, including cyber-bullying, cyber-stalking, and online harassment. Many international efforts have been invested in mandating laws and legislation in this regard. A federal law, the Children's Online Privacy Protection Act (FTC 1998), assists in protecting children younger than 13 when they are online by requiring websites to outline their privacy policies and obtain parental approval prior to gathering or using a child's personal information, such as name, address, phone number, or social security number. The goal of the Children's Internet Protection Act is to safeguard children from risky online experiences (FCC 2011). Schools or libraries must possess a safe Internet usage policy that filters or prevents access to media materials that are a considered harmful or a threat to children. This would qualify them to receive discounts for telecommunication services and internet access through the Universal Service Program for Schools and Libraries that is also known as E-rate. Legislation against cyber-stalking has been published by the Washington State Legislature (2004) as a good example for other G20 countries of the strategic and effective use of legislation.

Therefore, it is highly recommended that the G20 community assemble a cyber safety framework to describe cyber-crime violations and the actions that schools (and states) should take for their prevention. This could be done by consolidating relevant laws and proposing additional legislative guidelines to address the possible risks that children may encounter by using the internet. The G20 nations should also collaborate with law enforcement agencies around the globe to prosecute all those involved in violating the rights of children to safety and protection in cyberspace.

Conclusion

The percentage of children using the internet has increased dramatically over the past few years, and the amount of time they spend online continues to rise steadily. While the internet can bring significant benefits of knowledge, education, and development, it also exposes children to many risks including cyberbullying, violence, radicalization, terrorism, and others. Despite the efforts made by various international and regional organizations, which support government efforts in this area, major challenges remain unaddressed in several areas. Unless policies specifically address children's protection and safety online, there is a high risk of increasing security incidents and safety issues in the future. The G20 is the international organizing body that is best positioned to combine these efforts into a cohesive and integrated strategy for improving children's protection and safety online.

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

Burns, Tracey, and Francesca Gottschalk (eds). 2019. "Educating 21st Century Children: Emotional Well-being in the Digital Age." Educational Research and Innovation, OECD Publishing, Paris. https://doi.org/10.1787/b7f33425-en.

Business20. 2017. "Ensuring Inclusiveness in a Digitalized World." G20 insights. https://www.g20-insights.org/2017/06/12/ensuring-inclusiveness-digitalized-world

Carin, Barry. 2017. "G20 Safeguards Vulnerabilities of Digital Economy, with Financial Sector Focus." G20 Insights. https://www.g20-insights.org/policy_briefs/g20-safeguards-vulnerabilities-digital-economy-financial-sector-focus

Chand, Ashok. 2005. "Do You Speak English? Language Barriers in Child Protection Social Work with Minority Ethnic Families." The British Journal of Social Work 35 (6): 807–821.

Cyber Security Awareness Alliance. n.d. "Go Safe Online" Accessed Feb 19, 2020. https://www.csa.gov.sg/gosafeonline

DQ Institute. 2020. Child Online Safety Index. Accessed Feb 15, 2020. https://www.dqinstitute.org/child-online-safety-index

Federal Communications Commission (FCC). 2011. Children Internet Protection Act (CIPA). Accessed February 20, 2020. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Federal Trade Commission (FTC). 1998. Children Online Privacy Protection Rule (COPPA). Accessed February 20, 2020. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proce

Infosec. 2017. Security Awareness for Kids: Tips for Safe Internet Use. https://resources.infosecinstitute.com/security-awareness-kids-tips-safe-internet-use/#gref

ISC2. 2016. "Study on Grade 4-8 Internet Usage Indicates 40% Chat with Strangers." https://blog.isc2.org/isc2_blog/2016/04/kids-internet-usage-us.html1

Livingstone, Sonia, John Carr, and Jasmina Byrne. 2016. "One in Three: Internet Governance and Children's Rights." Innocenti Discussion Papers no. 2016-01, UNICEF Office of Research - Innocenti, Florence.

Livingstone, Sonia, Julia Davidson, Joanne Bryce, Saqba Batool, Ciaran Haughton, and Anulekha Nandi. 2017. “Children’s Online Activities, Risks and Safety: A Literature Review.” UKCCIS Evidence Group. London School of Economics and Political Science.

Morris, Emma. 2016. “Children: Extremism and Online Radicalization.” Journal of Children and Media 10 (4): 508–514. DOI: 10.1080/17482798.2016.1234736

National Cyber Security Authority. 2020. Riyadh Declaration for Cybersecurity. Global Cybersecurity Forum, Riyadh https://globalcybersecurityforum.com/declaration

OECD Council. 2012. Recommendation of the OECD Council on the Protection of Children Online Accessed February 2, 2020. https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf

Peter, Jochen, Patti M. Valkenburg, and Alexander P. Schouten. 2006. "Characteristics and Motives of Adolescents Talking with Strangers on the Internet." CyberPsychology & Behavior 9: 526–530.

Phippen, Andy. 2017. “Online Technology and Very Young Children: Stakeholder Responsibilities and Children’s Rights.” International Journal of Birth and Parent Education 5 (1): 29–32.

Raising Children Network, The. 2018. “Internet Safety for Children 6-8 years.” https://raisingchildren.net.au/school-age/play-media-technology/digital-safety/internet-safety-6-8-years

REMS TA Center. 2020. “Cyber Safety Consideration for K-12 Schools and School District.” Cyber Safety for Schools Fact Sheet. https://rems.ed.gov/docs/Cyber_Safety_K-12_Fact_Sheet_508C.PDF

Schwarzer, Johannes, Lurong Chen, Wallace Cheng, Dan Ciuriak, Fukunari Kimura, Junji Nakagawa, Richard Pomfret, and Gabriela Rigoni. 2019. “The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies.” G20 Insights. https://www.g20-insights.org/policy_briefs/the-digital-economy-for-economic-development-free-flow-of-data-and-supporting-policies

UNICEF. 2016. “Children’s Rights and the Internet: From Guidelines to Practice.” United Nations Children’s Fund (UNICEF) and The Guardian. https://www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf

UNICEF. 2018. “More than 175,000 Children go Online for the First Time every Day, Tapping into Great Opportunities, but Facing Grave Risks: On Safer Internet Day, UNICEF calls for urgent action to protect Children and their digital footprint.” Press Release. https://www.unicef.org/eca/press-releases/more-175000-children-go-online-first-time-every-day-tapping-great-opportunities

UNICEF. 2020. “Children at Increased Risk of Harm Online during Global COVID-19 Pandemic: Newly released technical note aims to help governments, ICT companies, educators and parents protect children in lockdown.” Press Release.

https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic

Vandoninck, Sofie, Leen d'Haenens, Rozane De Cock, and Verónica Donoso. 2011. "Social Networking Sites and Contact Risks among Flemish Youth." Childhood 19(1): 69–85. https://doi.org/10.1177/0907568211406456

Washington State Legislature. 2004. Cyberstalking, RCWs, Title 9, Chapter 9.61, Section 9.61.260. Accessed March 2, 2020. https://app.leg.wa.gov/RCW/default.aspx?cite=9.61.260

WeProtect Global Alliance. 2020. "Impact of COVID-19 on Online Child Sexual Exploitation." https://www.weprotect.org/products

AUTHORS

Muhammad Khurram Khan
King Saud University

Omaimah Bamasag
University of Jeddah

Abdullah Ayed Algarni
Institute of Public Administration

Mohammad Alqarni
University of Jeddah