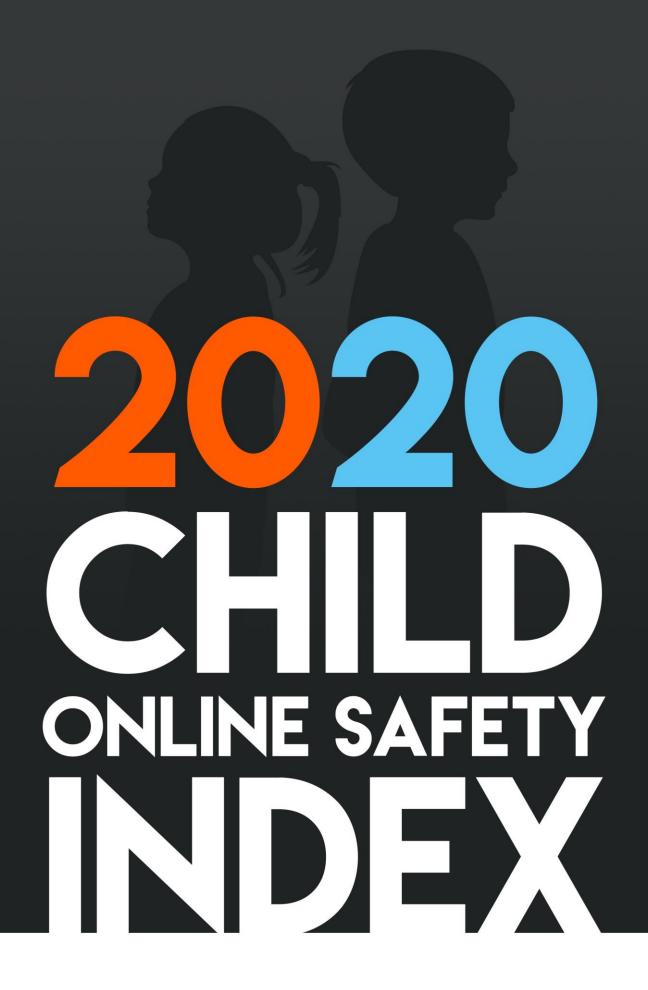
A FINDINGS AND METHODOLOGY REPORT BY:





#### DQ INSTITUTE TERMS OF USE AND DISCLAIMER

The analysis presented in the 2020 Child Online Safety Report (the "Report") integrates several methodologies from international organizations, universities, and corporations with proprietary analysis. The Report presents information that was compiled and/or collected by the DQ Institute (all information is referred herein as "Information"). Information in this Report is subject to change without notice. Other parties may have ownership interests in some of the Information contained in this Report. The DQ Institute in no way represents or warrants that it owns or controls all rights in all information, and the DQ Institute will not be liable to users for any claims brought against users by third parties in connection with their use of any information. The DQ Institute, its agents, officers, and employees do not endorse or in any respect warrant any third-party products or services by virtue of any information, material, or content referred to or included in this Report. Users shall not infringe upon the integrity of the information and in particular shall refrain from any act of alteration of the information that intentionally affects its nature or accuracy. If the information is materially transformed by the user, this must be stated explicitly along with the required source citation. For information compiled by parties other than the DQ Institute, users must refer to those parties' terms of use, in particular concerning the attribution, distribution, and reproduction of the information. When information for which the DQ Institute is the source and such information is distributed or reproduced, it must appear accurately and be attributed to the DQ Institute. This source attribution requirement is attached to any use of information, whether obtained directly from the DQ Institute or from a user. Users who make DQ Institute available to other users through any type of distribution or download environment agree to make reasonable efforts to communicate and promote compliance by their end users with these terms. Users who intend to sell DQ Institute information must first obtain permission from the DQ Institute.

#### **RESEARCHERS:**

Yuhyun Park, PhD – Founder, DQ Institute

Douglas A. Gentile, PhD – Lead Researcher, Professor at Iowa State University

James Morgan, PhD – Researcher, DQ Lab Pte Ltd

Lanmiao He, MS – Researcher, PhD Candidate at Iowa State University

Johnie J. Allen, MS – Researcher, PhD Candidate at Iowa State University

Seung Min Jung – Data Scientist, DQ Lab Pte Ltd

Jallene Chua – Researcher, DQ Lab Pte Ltd

Adrian Koh – Junior Data Scientist, DQ Lab Pte Ltd

Copyright © DQ Institute 2020. All rights reserved.

The Report and an interactive online platform are available at: www.dqinstitute.org/child-online-safety-index

CONTACT@DQINSTITUTE.ORG

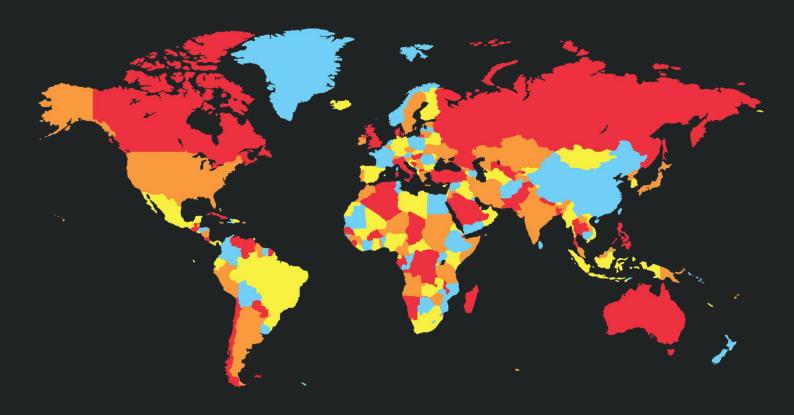
Web: www.dqinstitute.org

### **CONTENTS**

About the 2020 COSI	5
The COSI Framework	8
Insights from the Index	10
2020 COSI Ranking	10
Children Facing Serious Cyber Risks	12
Mitigating Cyber Risks Starting with Disciplined Technology Use	15
Digital Competency Minimizes Risks and Maximizes Potential	16
Parents and Teachers Matter	19
Governments and Industry are Responsible	20
Countries' Performance on 6 Pillars	22
National Reports	25
Australia	26
China	27
Colombia	28
Dominican Republic	29
Ecuador	30
Egypt	31
Hong Kong	32
India	33
Indonesia	34
Italy	35
Japan	36
Republic of Korea	37
Malaysia	38
Mexico	39
Nepal	40
New Zealand	41
Nigeria	42
Oman	43
Peru	44

Philippines	45
Saudi Arabia	46
Singapore	47
South Africa	48
Spain	49
Thailand	50
Turkey	51
United Kingdom	52
United States	53
Uruguay	54
Vietnam	55
Research Methods	56
The Index Development	56
Pillar 1: Cyber Risks	56
Area 1: Cyberbullying	56
Area 2: Disordered Use of Technology	57
Area 3: Risky Content	59
Area 4: Risky Contacts	62
Area 5: Cyber Threats	63
Area 6: Reputational Risks	64
Pillar 2: Disciplined Digital Use	67
Area 7: Excessive Screen Time	67
Area 8: High Social Media and Gaming Activity	68
Area 9: Mobile Ownership for Children	69
Pillar 3: Digital Competency	71
Area 10: Digital Citizen Identity	72
Area 11: Screen Time Management	72
Area 12: Cyberbullying Management	73
Area 13: Cyber-Security Management	74
Area 14: Digital Empathy	75
Area 15: Digital Footprint Management	76
Area 16: Critical Thinking	77
Area 17: Privacy Management	78

Pillar 4: Guidance and Education	80
Area 18: Parental Guidance	80
Area 19: Online Safety Education	81
Pillar 5: Social Infrastructure	82
Area 20: Legal Framework	82
Area 21: Cyber Security Infrastructure	84
Area 22: Industry and Civic Engagement	85
Pillar 6: Connectivity	89
Area 23: Access	89
Area 24: Speed	90
Data and Methodology	91
Data Collection	91
Research Procedure	91
Sample Size	92
Computation of Scores	93
Adjustment Based on Age Group and Data Sources	93
Limitations	94
References	95



### **ABOUT THE 2020 COSI**

### REAL-TIME MEASURE FOR CHILD ONLINE SAFETY

Two years ago, on Safer Internet Day (6th February 2018), the 2018 DQ Impact Report was published in association with the World Economic Forum. That initial report examined online safety and digital citizenship among 38,000 8- to 12-year-olds across 29 countries. Our key finding at that time was that 56% of children were exposed to at least one cyber risk (including risks like cyberbullying, gaming disorder, offline meeting with strangers, and online sexual behaviors). This report (available at <a href="https://www.dqinstitute.org/2018dq\_impact\_report/">https://www.dqinstitute.org/2018dq\_impact\_report/</a>) created an impetus to expand and deepen our knowledge of the risks children face, as well as what resources act as protective factors.

In the two years following, we have broadened our vision and increased our measurements to examine six major pillars of support for children's online safety (see details below). This report compares the results across 30 countries, and includes data from over 145,426 children, as well as from other external sources such as the International Telecommunication Union (ITU), Global System for Mobile Communications Association (GSMA), Economist Intelligence Unit, and others.

Although there are many positive and promising results from this broad look across countries, it is still the case that far too many children are exposed to potentially serious risks.

#### WHAT IS THE COSI?

The Child Online Safety Index (COSI) is the world's first real-time analytic platform to help nations better monitor the status of their children's online safety.

The COSI is based on six pillars which form the COSI framework. Pillars one and two, Cyber Risks and Disciplined Digital Use, relate to Wise Use of digital technology. Pillars three and four, Digital Competency and Guidance & Education, are related to Empowerment. The final two pillars relate to Infrastructure, these are the pillars of Social Infrastructure and Connectivity.

Through the index, nations will be able to identify areas of improvement for their children's online safety issues across the six pillars. Global benchmarking will make targeting those areas more effective, and improve deployment of relevant programs and initiatives. Actors can then effectively coordinate efforts to enhance child online safety and digital citizenship within their nations, with the ability to measure national progress.

By being linked with DQ assessment tools and its global database, the COSI will be automatically updated as nations progress with their initiatives to improve child online safety.

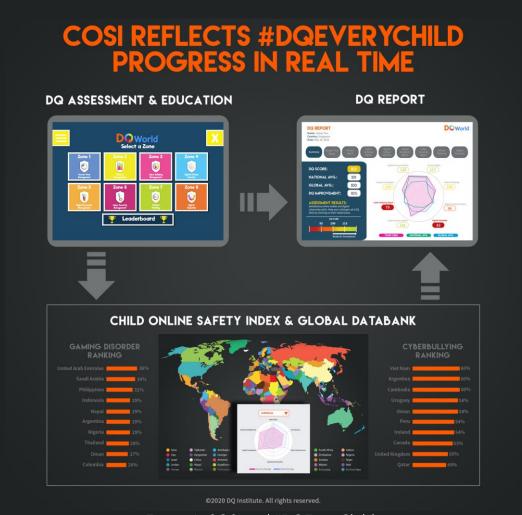


Figure 1: COSI and #DQEveryChild

This 2020 COSI Findings and Methodology Report summarizes the key findings by reporting in-depth analyses and research as well as providing a detailed methodology.

### **#DQEVERYCHILD - A GLOBAL DIGITAL CITIZENSHIP MOVEMENT SINCE 2017**

The 2020 COSI data were collected from 145,426 children and adolescents in 30 countries from 2017-2019 as part of #DQEveryChild. The COSI is the culmination of three years of #DQEveryChild, a strategic global movement aiming to empower children with comprehensive digital citizenship competencies from the start of their digital lives using the online education and assessment program DQ World. The movement started in Singapore with the support of Singtel and has quickly expanded in collaboration with the World Economic Forum to include over 100 partner organizations.

### DQ COMPETENCY FRAMEWORK AS GLOBAL STANDARDS FOR DIGITAL LITERACY, SKILLS, AND READINESS

In September 2018, the DQ Framework – called DQ Global Standards – was officially announced as the common language for digital literacy, skills, and readiness by the Coalition for Digital Intelligence (CDI) whose members include the Organization for Economic Cooperation and Development (OECD), IEEE SA, and DQ Institute. Beyond existing measures

comprehensive set of digital competencies that enables individuals to thrive in the digital economy. Its common framework is based on aggregating more than 25 world-leading frameworks about digital literacy, skills, and readiness. With

the support of CDI, DQ Global Standards are becoming a key reference for building next-generation global standards across the educational and technology sectors in order to promote children's digital literacy as well as for supporting digital skills training for the global workforce.

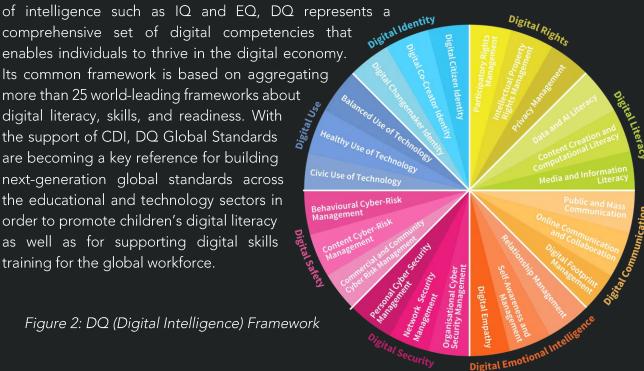


Figure 2: DQ (Digital Intelligence) Framework

### THE COSI FRAMEWORK

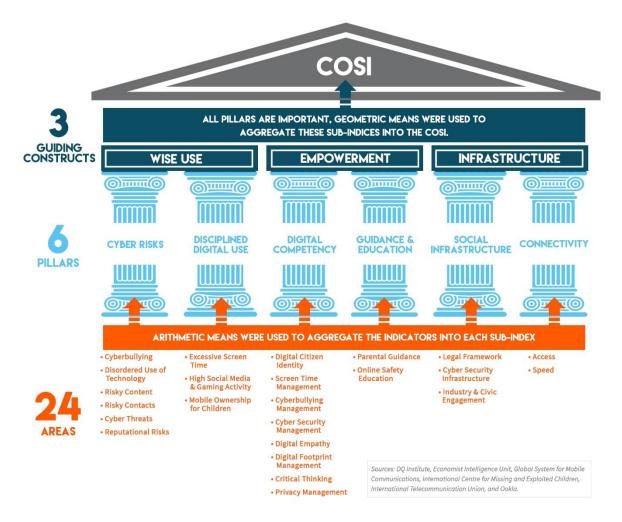


Figure 3: The COSI Framework

We believe that a nation's basic digital readiness starts from ensuring the safety of children online. The 2020 Child Online Safety Index (COSI) measures the level of online safety for children in 30 countries. Child online safety can be explained at three hierarchical levels. At the highest level are three guiding constructs: Wise Use, Empowerment, and Infrastructure. Each guiding construct is based on two pillars and each of those pillars is based on two to eight areas. Areas, in turn, are based on multiple indicators.

#### **WISE USE**

The first guiding construct of the COSI is Wise Use, which accentuates the benefits and minimizes the risks associated with cyberspace. Wise Use begins with the pillar of Cyber Risks. This pillar is based on children's exposure to the following cyber risks: Cyberbullying, Disordered Use of Technology, Risky Content, Risky Contacts, Cyber Threats, and Reputational Risks. The next pillar is Disciplined Digital Use, which examines: Excessive Screen

Time, High Social Media & Gaming Activity, and Mobile Ownership for Children. These measures indicate internet usage that could be characterized as disciplined or controlled. For instance, mobile usage is empirically riskier because using the internet in this way is more difficult to supervise. Disciplined Digital Use is hypothesized to be a protective factor that limits children's Cyber Risks.

#### **EMPOWERMENT**

The next guiding construct is Empowerment. The first pillar of Empowerment refers to Digital Competency, which is based on eight areas: Digital Citizen Identity, Screen Time Management, Cyberbullying Management, Cyber Security Management, Digital Empathy, Digital Footprint Management, Critical Thinking, and Privacy Management. Children with high levels of Digital Competency can successfully negotiate the online world to reap the benefits while being mindful to protect themselves from risks. The fourth pillar is Guidance & Education from schools and parents. This pillar can give children the knowledge and skills needed to safely navigate the online world and thus supports Digital Competency.

#### **INFRASTRUCTURE**

The first pillar of Infrastructure is Social Infrastructure. This is based on the presence of Legal Frameworks, Cyber Security Infrastructure, and Industry Engagement. The final pillar is Connectivity, which is a composite of scores relating to the proportion of children who have Access to the internet and the Speed of internet connections. Connectivity is necessary for children to realize the benefits of the online world but also has the potential to expose children to online harms. The presence of high levels of Social Infrastructure can mitigate these risks and create conditions for Empowerment.

#### **AIMS**

The overarching aim of the COSI is to ensure strong and improving performance on each of the six pillars. Providing a standard metric across countries can encourage stakeholders to work together to bring about positive changes and to maintain best practices.

The following section reports detailed analyses that can aid stakeholders in realizing the aims of DQ to improve child online safety worldwide. Analyses provide information on how to prioritize and focus efforts for the prevention of online harm. The results are relevant for parents, educators, paediatricians, and policymakers.

COSI scores allow for comparisons between countries, highlighting the urgency for targeted action within and across countries.

### **INSIGHTS FROM THE INDEX**

### 2020 COSI RANKING

COSI scores were computed in a relativistic manner, meaning that the final COSI score is not a simple tallying up of frequencies. Scores were standardized across the 30 countries and transformed into percentiles. For instance, Spain's score of 75.6 does not mean that the task of child online safety is three quarters complete, it means that their results across a number of indicators were higher than other nations (they are at an average of the 76<sup>th</sup> percentile across multiple indicators, relative to the other 29 countries in this sample). Likewise, Thailand's score of 10.5 does not mean that the country has danger rates of 89.5, rather it reflects a degree of difference with the performances of other nations (Thailand's average percentile is 10<sup>th</sup> across the multiple COSI indicators, relative to the other 29 countries).



Figure 4: Global Ranking of the 2020 COSI

Scores can be classified as below average, average or above average. COSI scores up to 29.9 were classified as below average, scores from 30 to 59.9 were classified as average, and scores of 60 and above were classified as above average. This is done to help readers interpret the COSI score. However, for a full understanding of the situation regarding child safety online readers should look beyond the overall COSI score and pay attention to performance in Pillars and Areas. These scores most precisely suggest priorities for improvement.

A note should also be made regarding sampling. Data were primarily gathered via schools. Countries in Figure 4 below which are marked with an asterisk had a disproportionate number of responses from children attending private, elite, or international schools. Findings from these countries should be interpreted with extra caution, as they may be less representative.

As can be seen from Figure 4, Spain achieved the top ranking with a score of 75.6. Five other countries also recorded an above average COSI score, these were Australia, Malaysia, Singapore, The Republic of Korea, and Italy. The majority of countries, 16 out of 30, were classified as having an average score. Italy, Japan, Turkey, India, China, New Zealand and the United States of America were towards the higher end of those classified as average since their scores were above 50. The remaining countries whose COSI score was classed as average were South Africa, Ecuador, Peru, Hong Kong, Egypt, Nigeria, The United Kingdom, Colombia, Mexico and the Dominican Republic. Eight countries were classified as having a below average score, these were the Philippines, Oman, Saudi Arabia, Indonesia, Uruguay, Vietnam, Nepal and Thailand.

### **REGIONAL ANALYSIS**

Nations were clustered into five groups, categorized by regional, economic and cultural factors. Southeast and South Asian countries included Indonesia, Malaysia, Nepal, Philippines, Thailand, Vietnam, India, and Singapore. Latin American countries included Colombia, Dominican Republic, Ecuador, Mexico, Peru, and Uruguay. Western countries included those located in Europe which were Italy, Spain, Turkey and the United Kingdom. This group also included Australia, New Zealand and the United States. Middle East and African countries included Egypt, Nigeria, Oman, Saudi Arabia, and South Africa. Finally, East Asian countries included China, Hong Kong, Rep. Korea, and Japan.

Figure 5 shows the average COSI sores for each region as well as the range in scores. Western Countries appeared strongest with scores ranging from 45.6 to 71.6 and a mean of 58.6. Next, East Asian countries showed a slightly lower mean and a narrower range. The mean was 54.3 and the range of scores was between 45.8 and 62.7. Southeast and South Asia ranged broadly, from 10.2 to 57.4 with a mean of 33.8. The Middle East and Africa and Latin America appeared to show similar performances, with respective means of 33.6 and 33.3. The range for Middle East and Africa was from 26.1 to 43.3, and for Latin America it was 24.5 to 42.1.

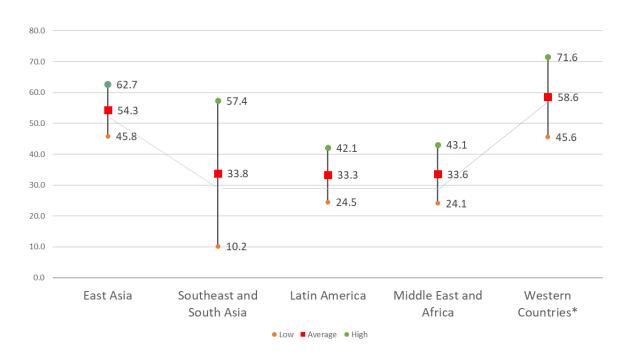


Figure 5: Regional Analysis of the 2020 COSI

### CHILDREN FACING SERIOUS CYBER RISKS

The 2018 DQ report 'Outsmart the Cyber-Pandemic: Empower Every Child with Digital Intelligence by 2020' found that more than half of 8- to 12-year-olds were exposed to cyber risks, such as cyberbullying, video game addiction, offline meetings, and online sexual behaviors. The report also identified risks to child online safety such as smartphone ownership, which increased the weekly screen time reported by children. It was found that 50% of children between the ages of 8-12 years accessed the internet through a smartphone and 85% used social media. Children who owned a smartphone and engaged in higher weekly screen time had a 70% chance of exposure to at least one Cyber Risk. This report found that on average children were spending 32 hours per week looking at a screen. Findings from 2020 COSI have not shown a radically different or improved situation.

Figure 6 depicts the proportion of children who are exposed to cyber risks across the full sample of over 145,000 children in 30 countries. The levels of cyber risk vary between the risk categories, but nonetheless, 8- to 12-year-olds appear likely to be exposed to several risks.

Parents are particularly likely to be concerned about their children meeting people offline whom they met online, with 17% of 8- to 12-year-olds acknowledging they have done this.

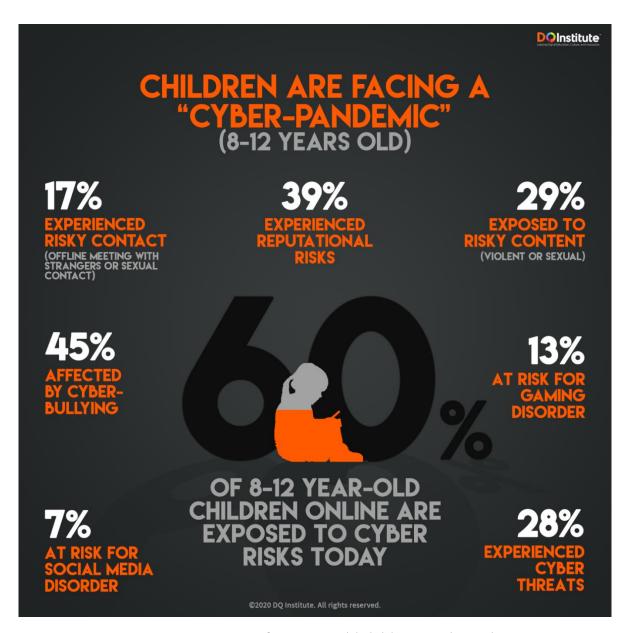


Figure 6: Exposure of 8-12 year-old children to cyber risks

Reputational Risks might take the form of a compromising or embarrassing photograph being shared online, with 39% reporting this.

Being Exposed to Risky Content can take the form of viewing sexual or violent media, with 29% admitting to this risk.

Gaming Disorder relates to using computer, console, and smartphone games in such a way that it causes significant disruption to their lives. 13% appear at risk for Gaming Disorder.

Similarly, Social Media Disorder is about dysfunctionality due to overuse of social media, with 7% at risk.

Cyber threats, such as phishing or hacking, were experienced by 28%.

Finally, 45% have been exposed to Cyberbullying, either as bullies themselves or as victims.

#### **REGIONAL DIFFERENCES**

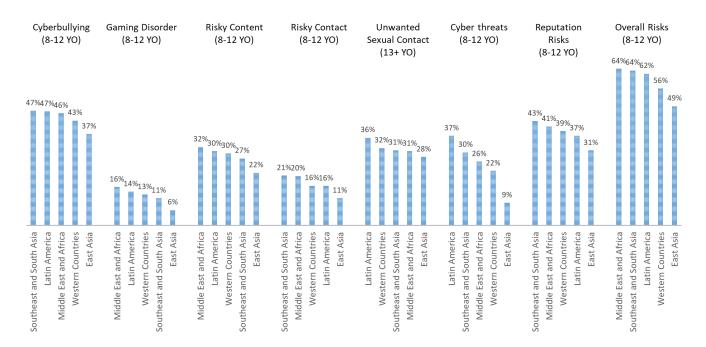


Figure 7: Exposure of children to various areas within cyber risks

Variations in levels of cyber risks were also apparent on a regional level, with these findings depicted in Figure 7.

Overall, 8- to 12-year-old children in East Asian countries had a 40% chance of being exposed to at least one Cyber Risk. For Western Countries the figure was 56%. In Latin American countries 62% of younger children experienced at least one risk. For both Middle East and African countries and Southeast and Southern Asian countries 64% of 8- to 12-year-old children reported at least one Cyber Risk.

The East Asian region recorded the lowest levels of risk across all risk categories. For the area of Cyber Threats amongst 8- to 12-year-olds, only 9% of those surveyed in East Asia had been exposed to this risk, for Latin America, the figure was 37%.

East Asian countries also appeared to be much safer than other regions in terms of Gaming Disorder for 8- to 12-year-olds, with 6% admitting to this risk. This compares favorably to all other regions whose frequencies ranged between 11% and 16%.

Looking to other indicators, the difference between the lowest and highest frequencies were not as large. Considering Cyberbullying of 8- to 12-year-olds, 37% of respondents in East Asia reported this risk whereas 47% of Southeast and South Asian and Latin American children did so.

The areas of Risky Content, Risky Contact, Unwanted Sexual Contact, and Reputational Risks followed a similar pattern. East Asia performed the best but differences between the highest

and lowest average frequencies were narrower than for the other risk categories, none were greater than 10%.

# MITIGATING CYBER RISKS STARTING WITH DISCIPLINED TECHNOLOGY USE

Disciplined Digital Use refers to use of online technologies in a way that mitigates the potential for harm. This pillar includes measurement across three areas: Excessive Screen Time, High Social Media and Gaming Activity, and Mobile Ownership at young ages. Lower levels of all three areas are positive examples of Disciplined Digital Use.

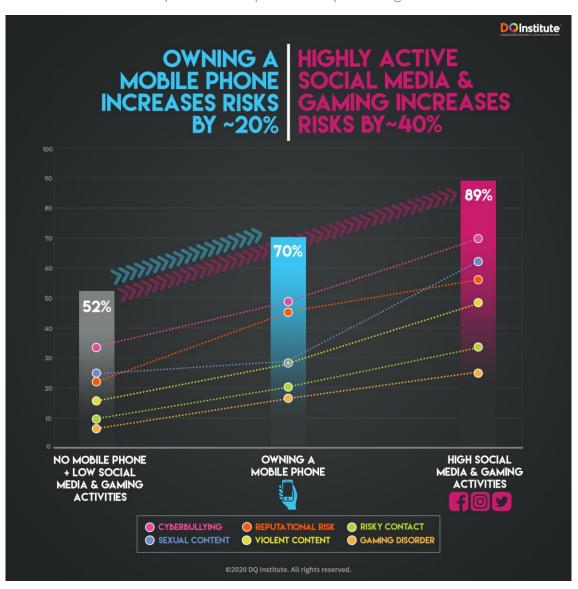


Figure 8: Effects of mobile phone ownership and level of social media & gaming activity on children's exposure to cyber risks

Figure 8 demonstrates the importance of Disciplined Digital Use. Children who do not own a smartphone have a 52% chance of experiencing one significant cyber risk. Children who own

a smartphone but do not report High Social Media and Gaming Activity have a 70% chance of experiencing a Cyber Risk category. Children who own a smartphone and report High Social Media and Gaming Activity have an 89% chance of exposure to at least one category of Cyber Risk. Disciplined Digital Use is encouraged because it is so strongly related to reduction in Cyber Risks.

# DIGITAL COMPETENCY MINIMIZES RISKS AND MAXIMIZES POTENTIAL

Digital Competency is a pillar of COSI which derives from the skills and knowledge provided by DQ World Digital Citizenship Education. Digital Competence allows children to minimize the risks and maximize the potential of the digital world. Rather than focusing on the prevention of specific risks, Digital Competency is designed as a holistic construct that should be applicable to all areas of online risks and potentials for benefit. Digital Competency is made up of eight areas.

The first area is Digital Citizenship, which refers to possessing a knowledge of the technologies that allows children to understand the distinctions and connections between the online and offline worlds. This allows children to use media effectively and securely.

Screen Time Management refers to personal decision making and self-control, especially regarding gaming behaviors. Children skilled in Screen Time Management are less at risk of Gaming Disorder.

Cyberbullying Management concerns skills and knowledge which help children to avoid bullying others online as well as being a victim of online bullying.

Cyber Security Management involves responsible decision making in the avoidance of cyber threats.

Digital Empathy refers to the ability to show empathy toward other people online as well as being aware of the impacts of their actions.

Digital Footprint Management refers to understanding the potential for reputational risks linked to social media use and the over sharing of personal information.

Critical thinking allows children to understand that not everything they read online will necessarily be true. Critical thinking also allows children to be selective and safe in choosing who they interact with online, preventing inappropriate sexual contacts as well as other risky contacts.

Privacy Management refers to the skills and knowledge needed to avoid placing oneself at risk from personal information shared online. This can relate to one's own privacy or the privacy of others.

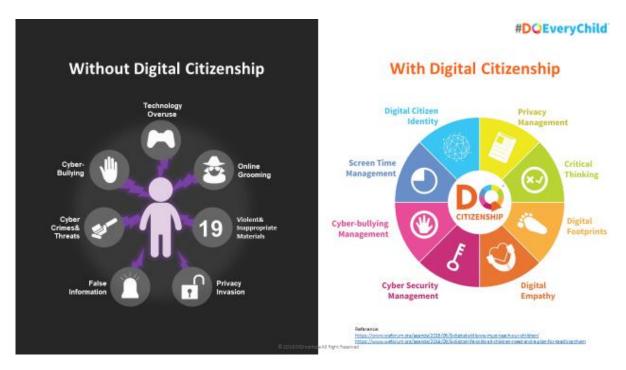


Figure 9: Risks and potentials for children without and with digital citizenship competency

DQ World Digital Citizenship Education can lead to improved outcomes in many areas. Comparing children who have and have not completed our DQ course, a number of benefits have been identified empirically (c.f., Figure 11).

Digital Citizenship has been shown to be particularly effective in stimulating safe and responsible attitudes and behaviors online. This has included more balanced screen time and improvements in self-control.

In addition, children who completed the course showed better understanding of online presence, privacy, and data protection as well as enhanced media and information literacies, high empathy, and global citizenship.

After completing the course, high levels of active parental mediation and school intervention were recorded.

These improvements then lead to better academic performance with enhanced future opportunities.

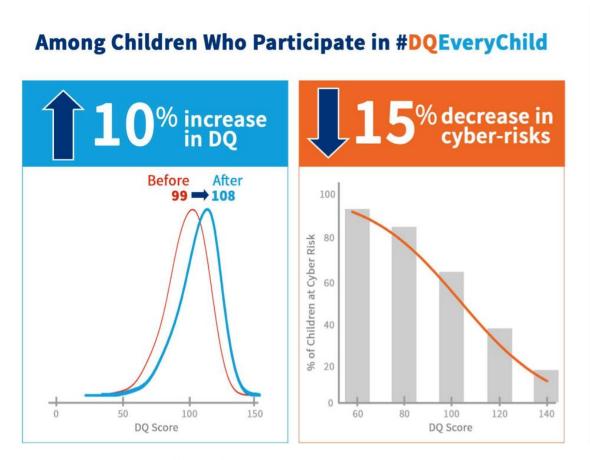


Figure 10: Effects of children's participation in #DQEveryChild

Figure 10 shows how partaking in DQ World Digital Citizenship Education that were used in #DQEveryChild can improve DQ scores and reduce Cyber Risks. Completing the course was associated with a 10% increase in DQ score which is the measure of digital citizenship. Higher DQ scores are linked with lower exposure to Cyber Risks. A 10% improvement on the DQ scale is associated with a 15% reduction in exposure to Cyber Risks.

#### PARENTS AND TEACHERS MATTER

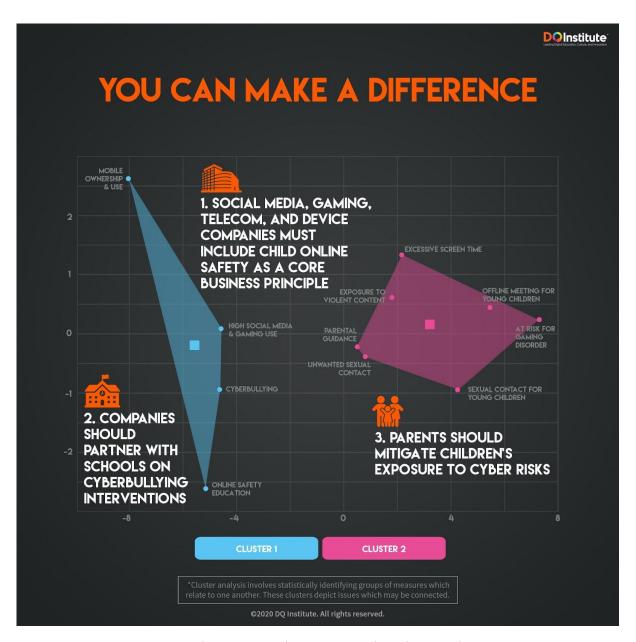


Figure 11: Clustering analysis across sub-indices in the COSI

The rich data gathered here allow us to examine patterns in risk and protective factors. A cluster analysis was conducted to identify how the various facets of the COSI relate to each other. Two clusters emerged that offer indications for how Cyber Risks can be prevented.

Cluster one features Online Safety Education, Mobile Ownership and Use, Excessive Social Media and Gaming Use, and Cyberbullying. Children who were high on one of these areas were more likely to be high on other areas of this cluster. The message from this is that if Cyberbullying is to be prevented, schools should ensure high levels of Online Safety

Education, parents should be empowered to avoid their children owning a smartphone and engaging in High Levels of Social Media and Gaming Use.

Cluster two contains Parental Guidance, Excessive Screen Time, being At Risk of Gaming Disorder, Offline Meeting for Young Children, Sexual Contact for Young Children (8-12) and Unwanted Sexual Contact for older children (13+). The message here is that low levels of Parental Guidance are related to a wide range of Cyber Risks.

Although analyses such as these cannot demonstrate causality, they support other studies that demonstrate how Parental Guidance can be key in preventing multiple harms. Governments, Telecommunications Companies, and Device Manufacturers must empower parents and schools to offer relevant education and guidance.

### **GOVERNMENTS AND INDUSTRY ARE RESPONSIBLE**

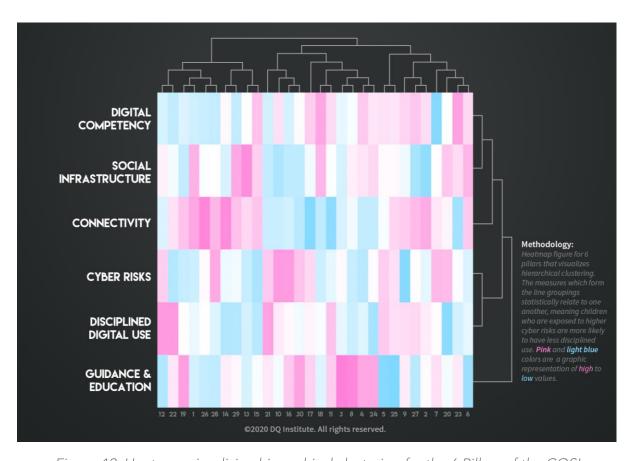


Figure 12: Heatmap visualizing hierarchical clustering for the 6 Pillars of the COSI

A combined cluster analysis and heat map revealed four themes in Figure 12.

First, Guidance & Education are closely linked to Disciplined Digital Use. This stands to reason, as Guidance and Education should stimulate Disciplined Digital Use. In addition, countries with strong policies and experience with the online world are likely to perform well in both areas.

Related to this, Connectivity also aligns with the clusters of Disciplined Digital Use and Guidance & Education. This is additional evidence that country-level policies are important.

Third, Cyber Risks are related to Disciplined Digital Use, which makes sense. Disciplined Use should lower risks, although it is also possible that a third variable may influence both.

Finally, Guidance and Education reveal themselves to be one of the likely third variables, as this pillar is associated with the cluster including both Cyber Risks and Disciplined Digital Use.

One take-away message is that both formal (e.g., through schools) and informal (e.g., via parents) digital literacy education is likely to be beneficial for reducing the risks that 8-12 year old children are exposed to online.

### **COUNTRIES' PERFORMANCE ON 6 PILLARS**

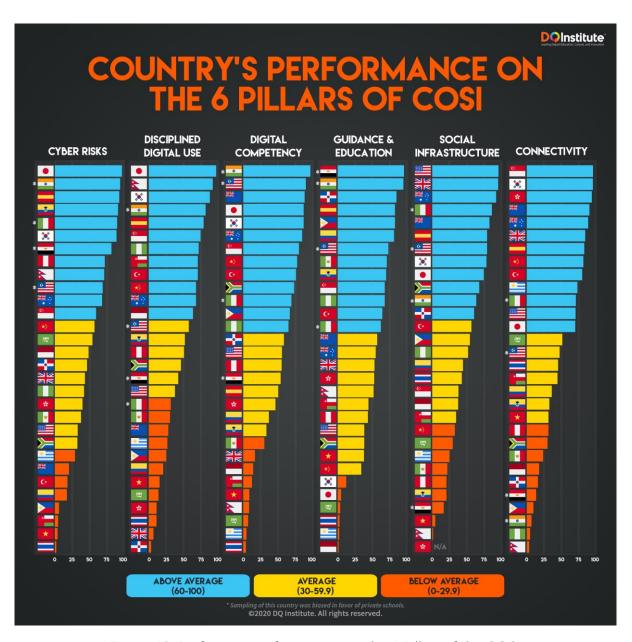


Figure 13: Performance of countries on the 6 Pillars of the COSI

Figure 13 shows the countries performance across the six pillars. As with the overall COSI scores performances on each of these pillars are also classified as below average if the country scored 29.9 or less, average if they scored between 30 and 59.9 and above average if they scored higher than 60.

As can be seen in the first columns, Japan recorded the highest scores for both Cyber Risks, with a score of 97.4. India (92.6), Spain (91.3), and Ecuador (90.4) all achieved high and similar scores (recall that a high score is always good in our scoring approach).

Japan (99.8) also achieved the highest score for Disciplined Digital Use. Nepal (96.6) and the Republic of Korea (89.8) should also be commended for their scores on this pillar.

India (98.8) scored highest on Digital Competency, nearly ten points higher than Malaysia (89.5) and Zealand (88.5) in second and third place.

India (95.9) also performed well in Guidance & Education coming second. Egypt (96.1) achieved the highest score for this category.

Regarding Social Infrastructure, as is also shown in Figure 14, below, Western Countries performed the strongest. The top five performing countries were The United States (96.5), United Kingdom (95.9), Australia (92.6), Italy (85.6), and New Zealand (81.4).

Connectivity is required for children to access the benefits of the online world while also being a necessary condition for Cyber Risks. Singapore (94.7) achieved the highest score in Connectivity, Republic of Korea (94.1) and Hong Kong (93.7) also scored highly.

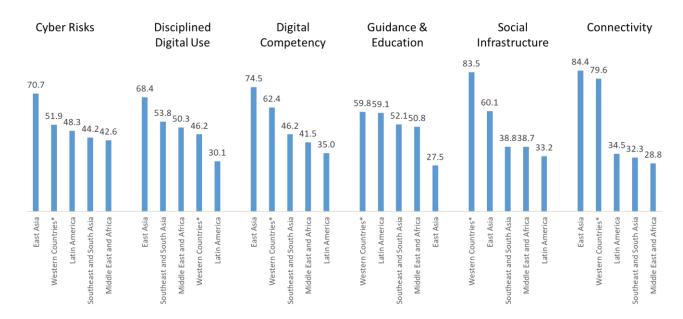


Figure 14: Performance of each cluster of nations on the 6 Pillars of the COSI

Performances across the six pillars were also compared by region. In Figure 15 Regions with the most positive scores for each pillar are shown on the left-hand side of the bar charts.

East Asia (70.7) has the best score for the pillar of Cyber Risks, nearly 20 points higher than Western Countries (51.9) who were awarded the second highest score.

East Asia (68.4) also had the best score for Disciplined Digital Use, almost 15 points ahead of Southeast and South Asia (53.8).

East Asia (74.5) was also dominant for the pillar of Digital Competency, 12.1 points higher than Western Countries (62.4).

Western Countries (59.8) and Latin America (59.1) recorded the highest average score for Guidance & Education. East Asia (27.5) recorded the lowest score for this pillar.

Western Countries (83.5) scored far in excess of any other region for the pillar of Social Infrastructure. East Asia (60.1) recorded the next highest score.

For connectivity Western Countries (84.4) and East Asian Countries (79.6) were again the highest performing regions.

# **NATIONAL REPORTS**

# **AUSTRALIA**

# Australia ranked 2<sup>nd</sup> out of 30 with an overall COSI score of 75.1

- Classified as an above average performance

#### Very strong in Social Infrastructure (3rd)

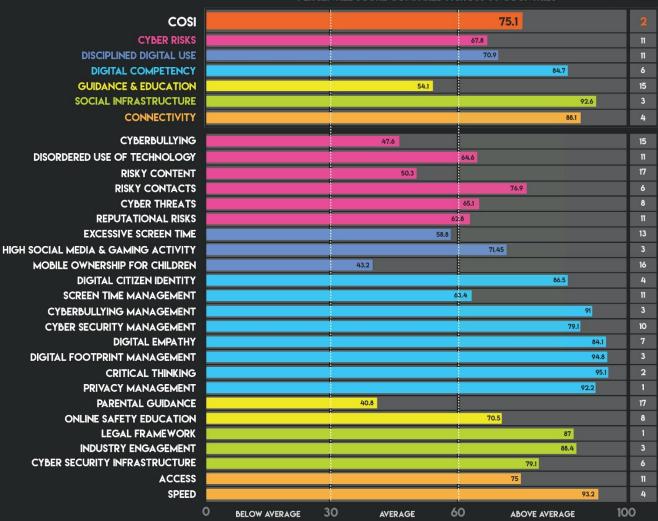
- Joint highest score in Legal Framework

#### Cyber Risks still present

- Children over 12 years old likely to be at risk for Cyberbullying (59.4%), Gaming Disorder (12.7%) and Exposure to Violent Content (38.2%)

#### Ranked 15th for Guidance & Education

– Improvement in this area could reduce Cyber Risks





# **CHINA**

# China ranked 10<sup>th</sup> out of 30 with an overall COSI score of 54.6

- Classified as an average performance

# Strong performances in Digital Competency (8th) and Connectivity (8th)

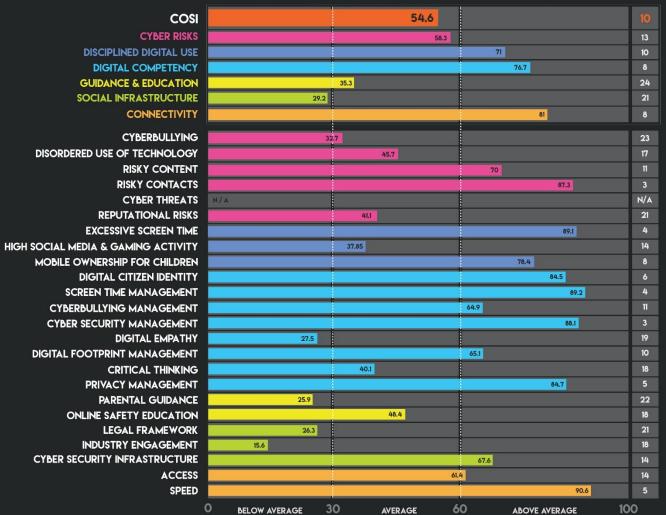
– Impressive score for Screen Time Management (4<sup>th</sup>)

# Low scores on Guidance & Education (24th) and Social Infrastructure (21st)

– These areas should be a priority for improvement

#### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES

RANK AMONG 30 COUNTRIES





### COLOMBIA

# Colombia ranked 20<sup>th</sup> out of 30, with an overall COSI score of 33.9

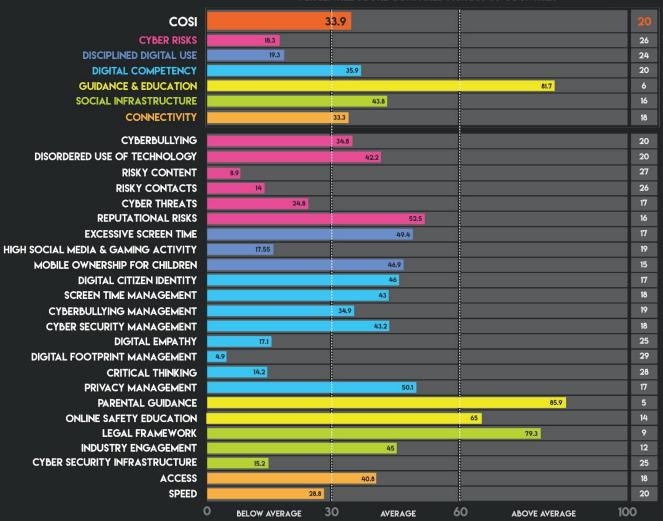
Classified at the lower end of an average performance

# Colombia scored low on the pillar of Cyber Risks (26<sup>th</sup>)

– Risky Content (27<sup>th</sup>) and Risky Contacts (26<sup>th</sup>) should be a priority

# Colombia is strong in Guidance & Education (6<sup>th</sup>)

– Cyber Security Infrastructure (25<sup>th</sup>) is an area where Colombia should seek to improve





### **DOMINICAN REPUBLIC**

The Dominican Republic was ranked 22<sup>nd</sup> out of 30, with an overall COSI score of 30.5

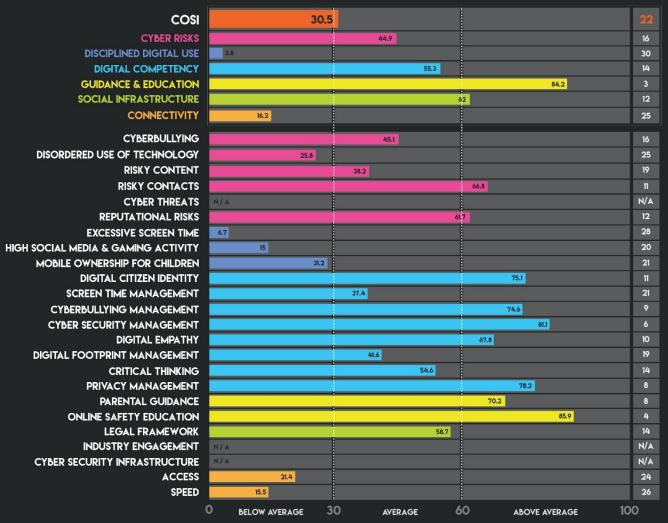
– This is classified at the lower end of an average performance

Very weak performance for the pillar of Disciplined Digital Use (30th)

Strong score for Guidance & Education (3rd)

The Dominican Republic could act by improving Connectivity (25<sup>th</sup>)

– Low scores for both Access (24<sup>th</sup>) and Speed (26<sup>th</sup>)





# **ECUADOR**

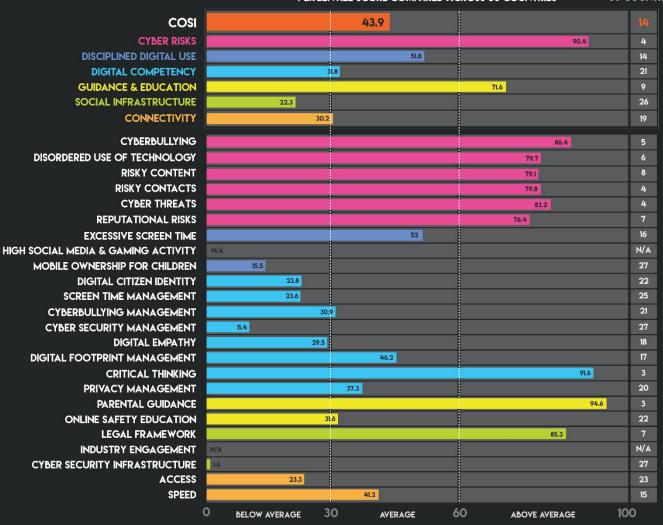
Ecuador ranks 14<sup>th</sup> out of 30 with an overall COSI score of 43.9

- This is classified as an average performance

Positive score for Cyber Risks (4th)

- Low levels of Cyberbullying (5th)

Cyber Security Management (27<sup>th</sup>) among children and Cyber Security Infrastructure (27<sup>th</sup>) also priorities for improvement





# **EGYPT**

# Egypt ranked 17<sup>th</sup> out of 30 with an overall COSI score of 40.1

- This is classified as an average performance

# Weak performance on Social Infrastructure (27<sup>th</sup>)

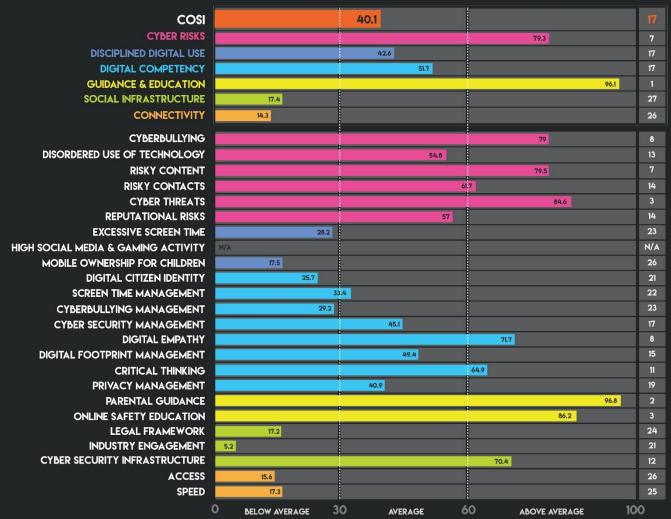
– Key areas for improvement are Legal Framework (24<sup>th</sup>) and Industry Engagement (22<sup>nd</sup>)

#### High score for Guidance & Education (1st)

– Both Parental Guidance (2<sup>nd</sup>) and Online Safety Education strong (3<sup>rd</sup>)

#### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES

RANK AMONG 30 COUNTRIES





# HONG KONG

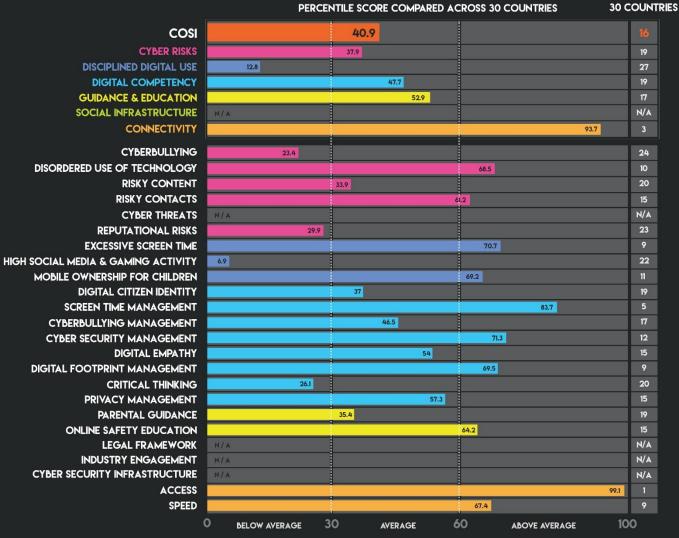
Hong Kong ranked 16th out of 30 on the overall COSI with a score of 40.9

- This is classified as an average performance

The results for Disciplined Digital Use (27th) were concerning

Low score for High Social Media and Gaming Activity (22<sup>nd</sup>)

Hong Kong was ranked 3rd for Connectivity and highest for Access (1st)



©2020 DO Institute. All rights reserved.

RANK AMONG



#### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES

RANK AMONG 30 COUNTRIES



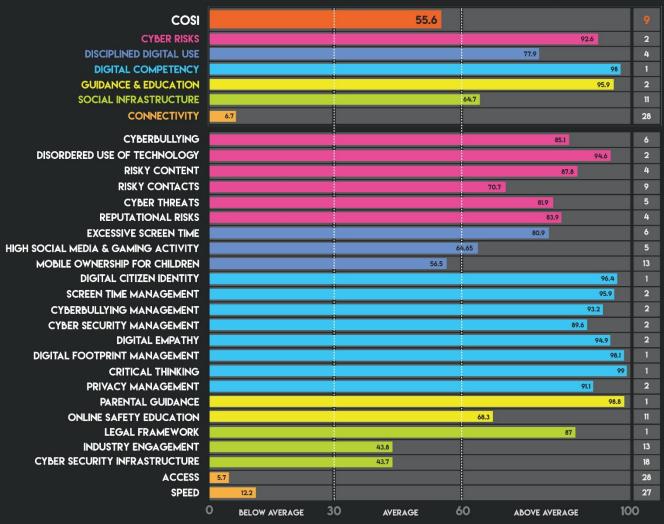
# India ranked 9<sup>th</sup> out of 30 with an overall COSI score of 55.6

- This is classified as an average performance

Scored very high for the pillars of Cyber Risks (2<sup>nd</sup>), Disciplined Digital Use (4<sup>th</sup>), Digital Competency (1<sup>st</sup>), and Guidance & Education (2<sup>nd</sup>)

### Low score for Connectivity (28th)

– Access (28<sup>th</sup>) to the internet and internet Speeds (27<sup>th</sup>) must be increased





# **INDONESIA**

# Indonesia ranked 26<sup>th</sup> out of the 30 with an overall COSI score 17.5

– This is a below average performance

#### Lowest score for Guidance & Education (30th)

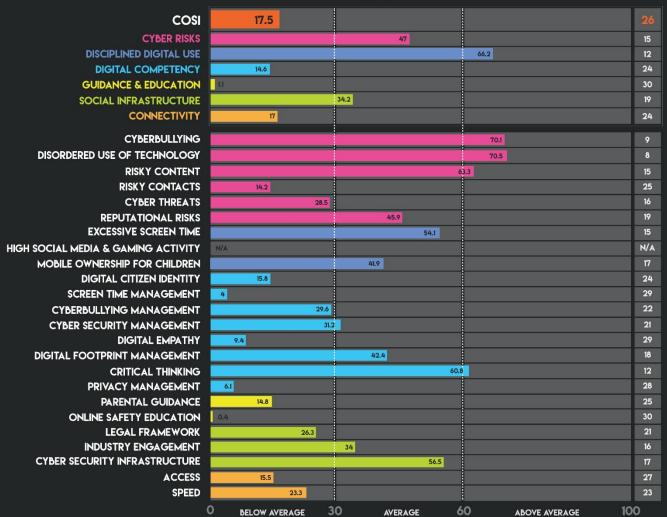
 Schools and families should be empowered to help guide children through the digital world

#### Indonesia low on Digital Competency (24th)

Weak performances for Screen Time
 Management (29<sup>th</sup>) and Digital Empathy (29<sup>th</sup>)

#### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES

RANK AMONG 30 COUNTRIES





### **ITALY**

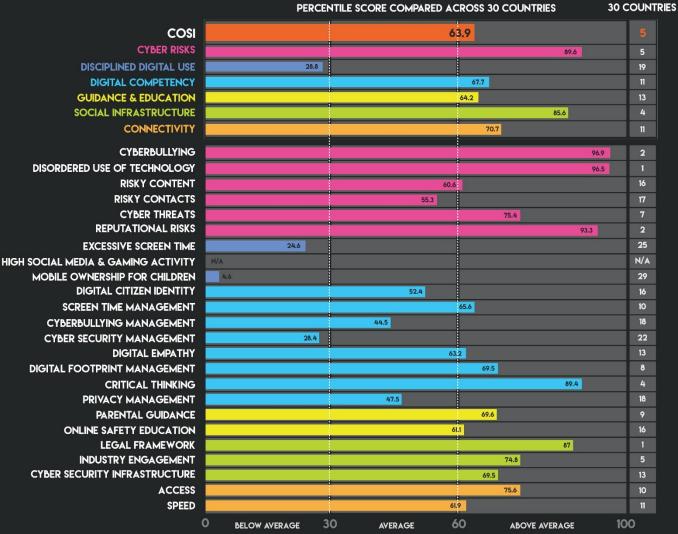
Italy ranked 5th out of 30 with an overall COSI score of 63.9

- Classified as an above average performance

#### Scored well for the pillars of Social Infrastructure (4th) and Cyber Risks (5th)

- Older children (13+) in Italy have the lowest risk of Cyberbullying (21.8%), Gaming Disorder (0.9%), and Social Media Disorder (0.9%) of any nations surveyed

**Problematic levels of Excessive Screen Time** (25th) and Mobile Ownership for Children (29th)



©2020 DO Institute. All rights reserved.

RANK AMONG

### **JAPAN**

Japan ranked 7<sup>th</sup> out of 30 with an overall COSI score of 57.6

- Classified as an average performance

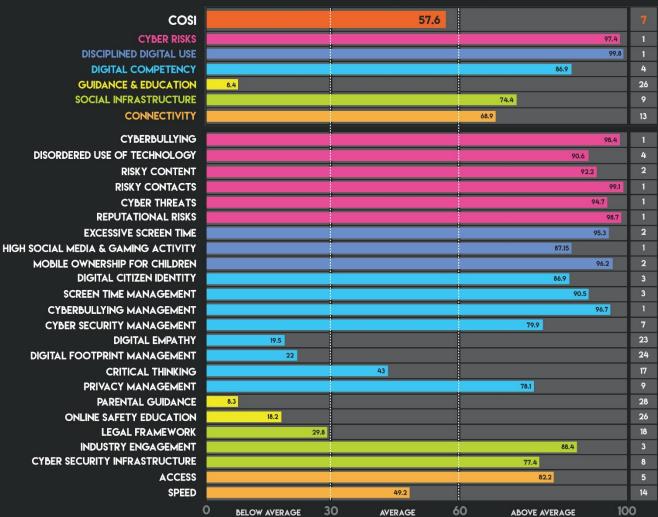
Japan was particularly strong in the areas of Disciplined Digital Use (1st) and Cyber Risks (1st)

However, Japan scored very low on Guidance & Education (26th)

– This is an area for improvement

The pillar of Connectivity (13th) could be improved

– Especially the area of Speed (14th)



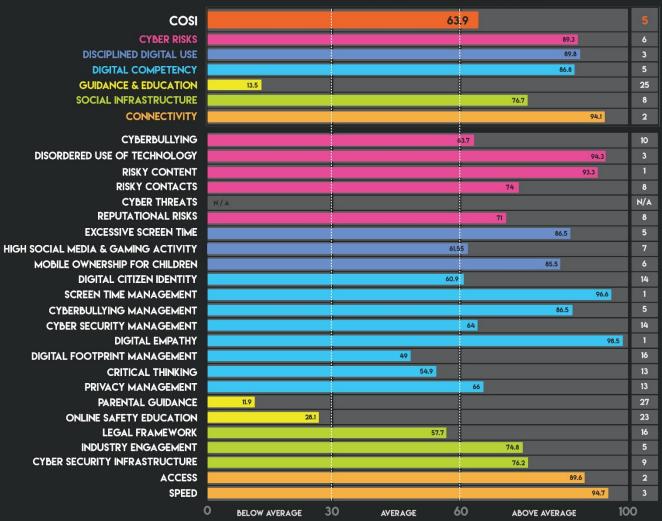
### **REPUBLIC OF KOREA**

The Republic of Korea ranked 5<sup>th</sup> out of 30 with an overall COSI score of 63.9

- An above average performance

Strong performances on Connectivity (2<sup>nd</sup>), Disciplined Digital Use (3<sup>rd</sup>), and Cyber Risks (6<sup>th</sup>)

An area for improvement is Guidance & Education (25<sup>th</sup>)





### Do Institute\* Leading Digital Education, Culture, and Innovation

## **MALAYSIA**

### Malaysia was ranked 3<sup>rd</sup> out of 30 with a COSI score of 68.1

- Classified as above average

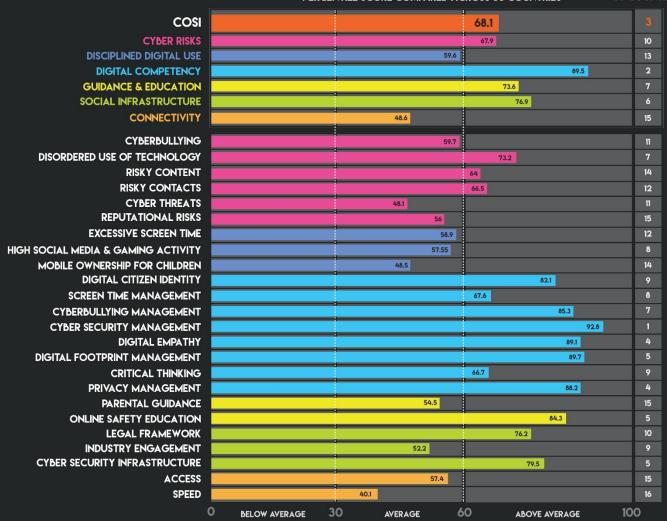
## Malaysia performed well on Digital Competency (2<sup>nd</sup>)

– Regarding children's Cyber Security Management (1<sup>st</sup>), Malaysia achieved the highest score

## Improvements can be sought for Disciplined Digital Use (13th)

– Malaysia ranked 12<sup>th</sup> for Excessive Screen Time and 14<sup>th</sup> on Mobile Ownership for Children

Connectivity (15<sup>th</sup>) could also be improved upon





## **MEXICO**

Mexico ranked 21<sup>st</sup> out of 30 with an overall COSI score of 32.8

- At the lower end of an average performance

Low scores for Social Infrastructure (24th) and Connectivity (23rd)

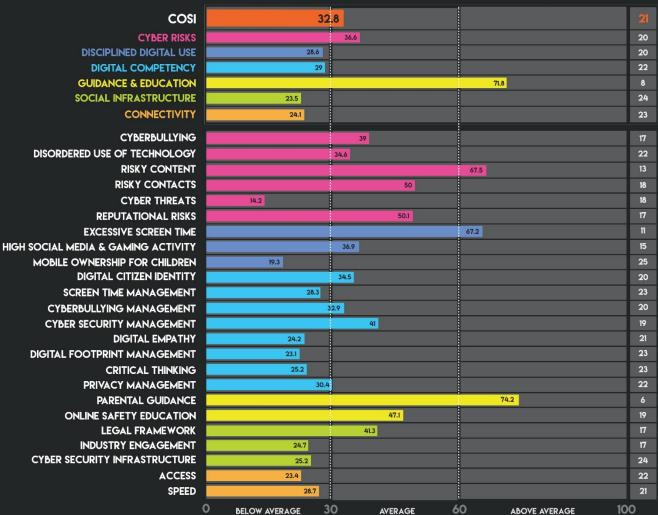
- Areas for improvement

Mexico enjoyed a good performance with regard to Guidance & Education (8th)

Despite this, Digital Competency (22nd) is low



RANK AMONG 30 COUNTRIES





### **NEPAL**

## Nepal ranked 29<sup>th</sup> out of 30 with an overall COSI score of 11.7

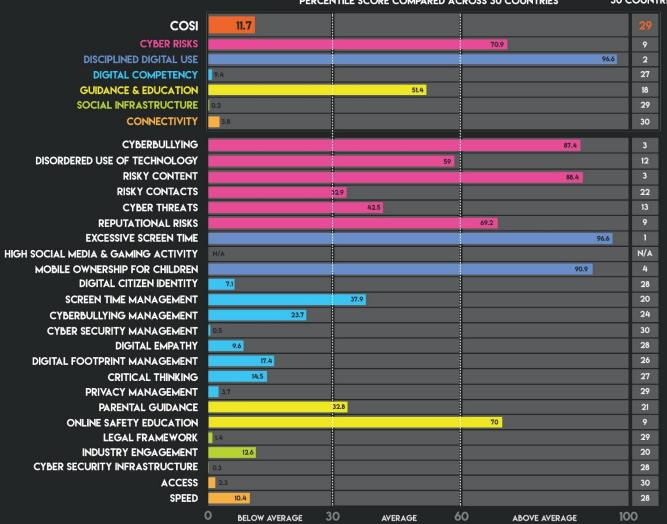
– This is classified as a below average performance

# Scored low on Connectivity (30<sup>th</sup>), Social Infrastructure (29<sup>th</sup>) and on Digital Competency (27<sup>th</sup>)

– Children in Nepal exhibited the lowest levels of Cyber Security Management (30<sup>th</sup>), Cyber Security Infrastructure (28<sup>th</sup>) was also the third lowest

## Strong on the pillar Disciplined Digital Use (2<sup>nd</sup>)

– Nepal scored highest for Excessive Screen Time (1<sup>st</sup>), meaning children were spending less time in front of screens



### **NEW ZEALAND**

New Zealand ranked 11<sup>th</sup> out of 30 with an overall COSI score of 52.1

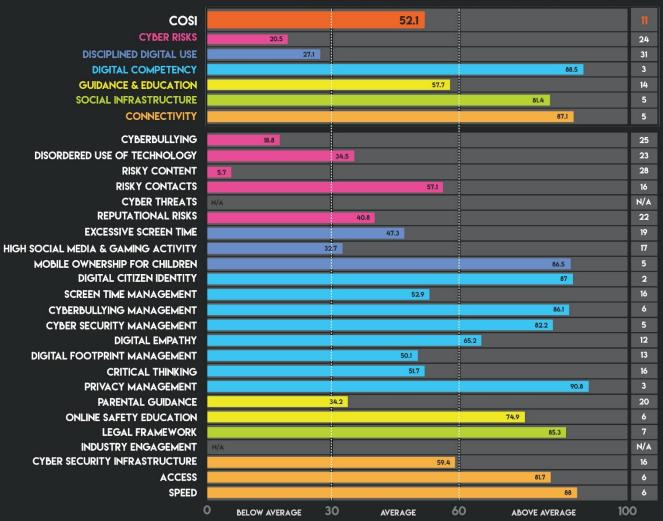
- This is classified as an average performance

New Zealand showed evidence of children being exposed to significant Cyber Risks (24<sup>th</sup>)

– Very low scores for Cyberbullying (25<sup>th</sup>) and Risky Content (28<sup>th</sup>)

However, children in New Zealand scored high for Digital Competency (3<sup>rd</sup>)

- Strong performances for Digital Citizen Identity (2<sup>nd</sup>) and Privacy Management (3<sup>rd</sup>)



#### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES

### **NIGERIA**

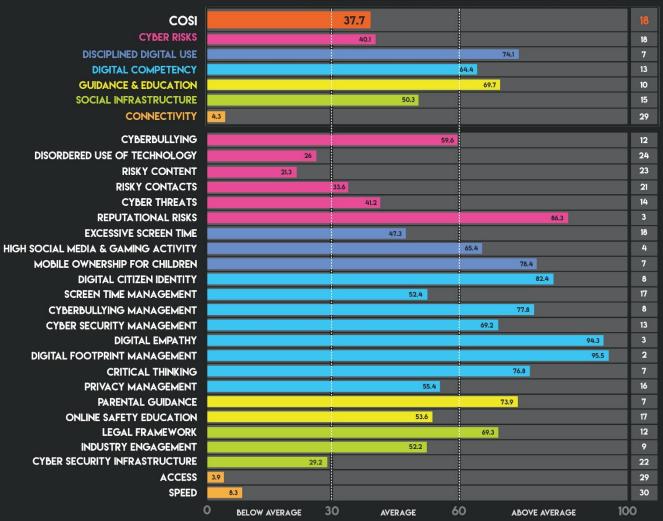
## Nigeria ranked 18<sup>th</sup> out of the 30 with an overall COSI score of 37.7

- Classified as being at the lower end of an average performance

#### Connectivity (29th) very low

 A clear area where improvement is needed to unlock the potential of the online world

Children surveyed in Nigeria were strong on Disciplined Digital Use (7th)



#### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES

#### RANK AMONG 30 COUNTRIES

### **OMAN**

## Oman ranked 24<sup>th</sup> out of 30 with an overall COSI score of 25.2

- A below average performance

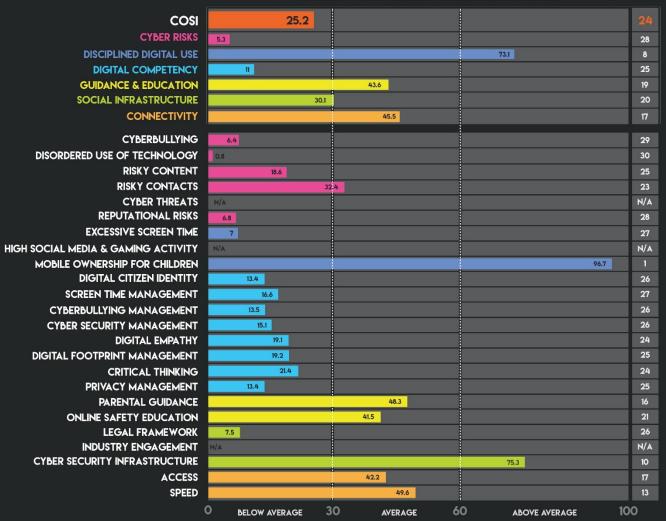
#### Very low score for Cyber Risks (28th)

– Especially low on Disordered Use of Technology (30<sup>th</sup>), Risky Content (25<sup>th</sup>) and Reputational Risks (28<sup>th</sup>)

## Strongest performance in Disciplined Digital Use (8th)

- Best score on Mobile Ownership for Children (1st)

Legal Framework (26th) a priority for improvement





### **PERU**

Peru ranked 15<sup>th</sup> out of 30 with an overall COSI score of 42.0

- An average performance

Mixed performance on Cyber Risks (8th) includes some positive findings

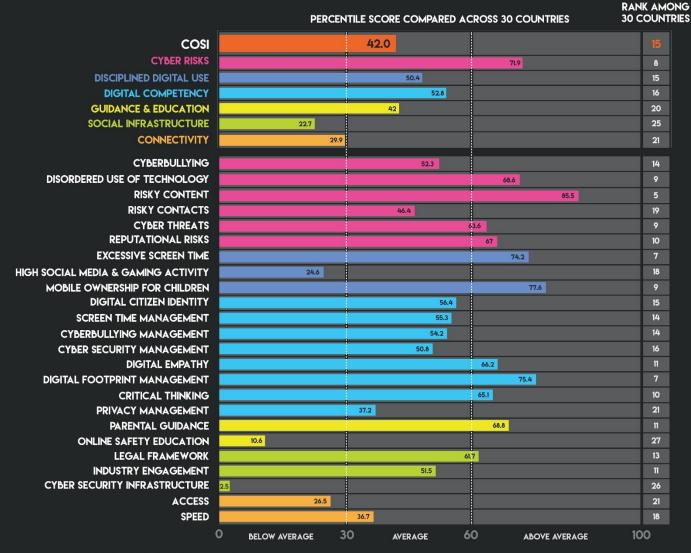
- Positive score on Risky Content (5th)

Social Infrastructure (25th) score concerning

– Very low for Cyber Security Infrastructure (26<sup>th</sup>)

Reasonable score for Parental Guidance (11th) but low for Online Safety Education (27th)

- This should be a priority for improvement



### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES RANK AMONG 30 COUNTRIES

### **PHILIPPINES**

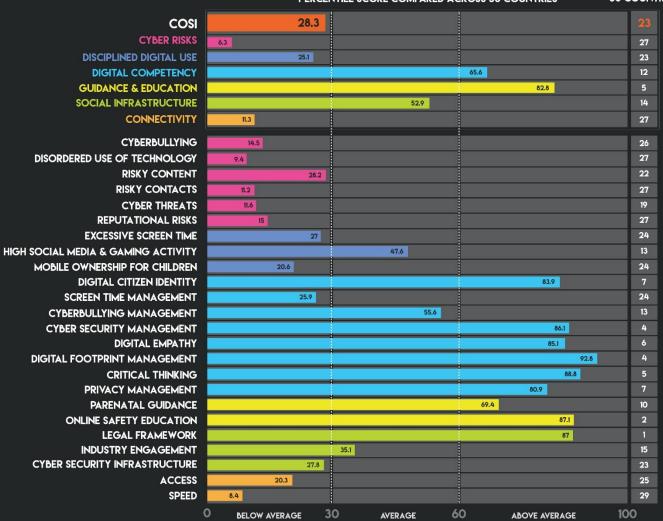
The Philippines ranked 23<sup>rd</sup> out of 30 with an overall COSI score of 28.3

- This was a below average performance

#### Very low score for Cyber Risks (27th)

– Especially for Cyberbullying (26<sup>th</sup>), Disordered Use of Technology (27<sup>th</sup>), Risky Contacts (27<sup>th</sup>), and Reputational Risks (27<sup>th</sup>)

The Philippines were strong in terms of Guidance & Education, showing the 5<sup>th</sup> highest score





### SAUDI ARABIA

### Saudi Arabia ranked 25<sup>th</sup> out of 30 with an overall COSI score of 19.8

- This was a below average performance

#### Low scores for Digital Competency (28<sup>th</sup>), Disciplined Digital Use (26<sup>th</sup>)

– Especially Screen Time Management (30<sup>th</sup>), Cyberbullying Management (27<sup>th</sup>), Digital Empathy (30<sup>th</sup>), and Digital Footprint Management (30<sup>th</sup>)

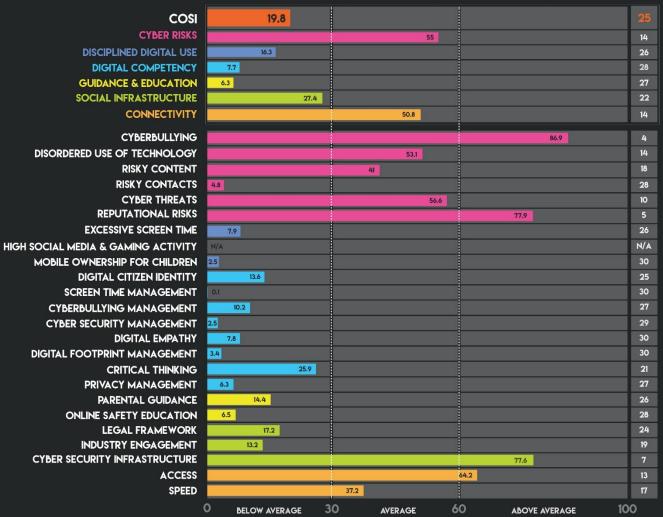
Improvements needed in Guidance & Education (27<sup>th</sup>)

#### Mixed score for Cyber Risks (14th)

– Positive rankings for Cyberbullying (4<sup>th</sup>) and Reputational Risks (5<sup>th</sup>)







#### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES

#### RANK AMONG 30 COUNTRIES

### **SINGAPORE**

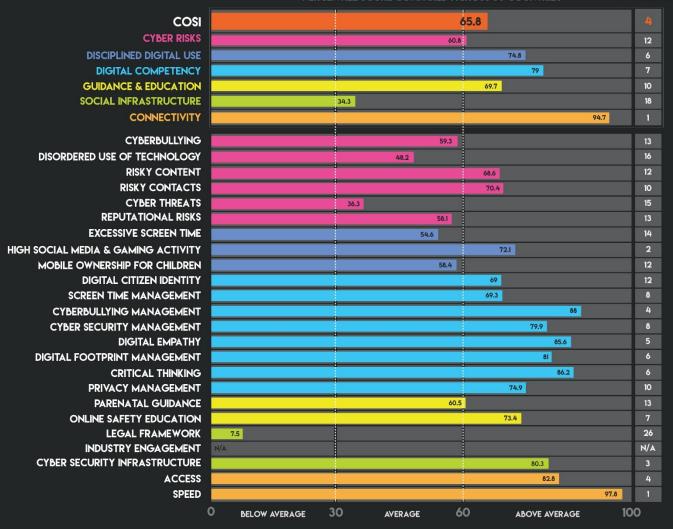
### Singapore ranked 4<sup>th</sup> out of 30 with an overall COSI score of 65.8

This was classified as an above average performance

Connectivity (1st) an especially strong area, with Singapore performing best

#### Work needed in Social Infrastructure (18th)

- Legal Framework (26th) scored very low





### **SOUTH AFRICA**

South Africa ranked 13th out of 30 with an overall COSI score of 45.1

This was classified as an average performance

Weaknesses were Cyber Risks (22<sup>nd</sup>), Guidance & Education (22<sup>nd</sup>), and Connectivity (22<sup>nd</sup>)

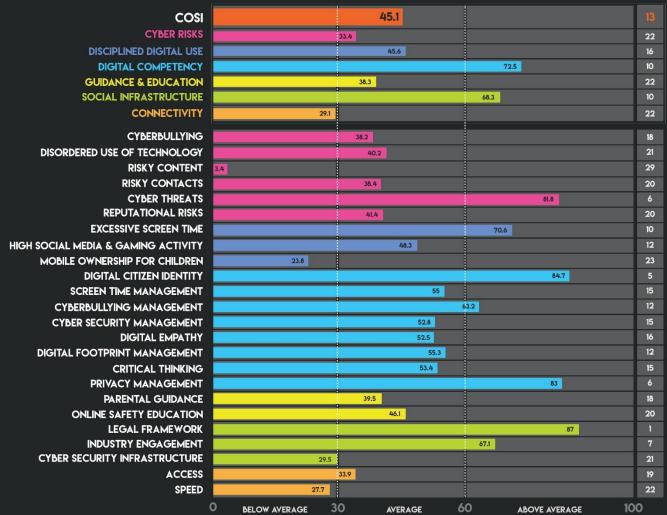
- Very low score for Risky Content (29th)

Digital Competency (10<sup>th</sup>) and Social Infrastructure (10<sup>th</sup>) were stronger areas

- High score for Legal Framework (1st)



RANK AMONG 30 COUNTRIES



### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES 30 COUNTRIES

### SPAIN

### Spain ranked 1<sup>st</sup> out of 30 with an overall COSI score of 75.6

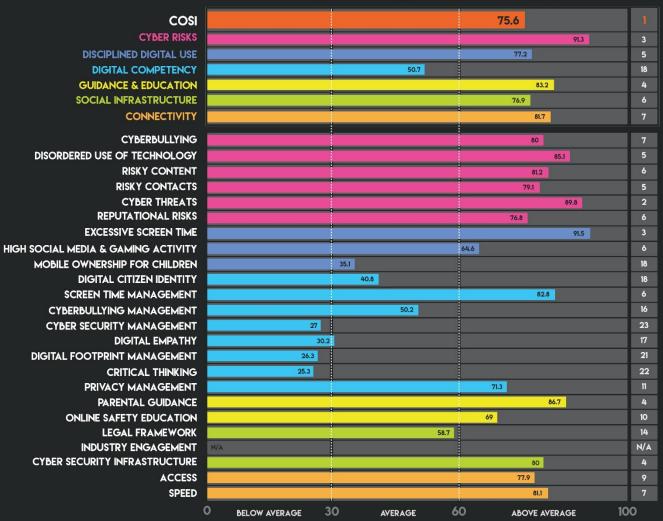
This was classified as an above average performance

#### High score for Cyber Risks (3rd)

– Especially in areas of Disordered Use of Technology (5<sup>th</sup>), Risky Contacts (5<sup>th</sup>), and Cyber Threats (2<sup>nd</sup>)

#### Some low scores for Digital Competency (18th)

Cyber Security Management (23<sup>rd</sup>),
 Digital Footprint Management (21<sup>st</sup>), and
 Critical Thinking (22<sup>nd</sup>)



#### PERCENTILE SCORE COMPARED ACROSS 30 COUNTRIES

#### RANK AMONG 30 COUNTRIES



## Thailand ranked last out of 30 with an overall COSI score of 10.5

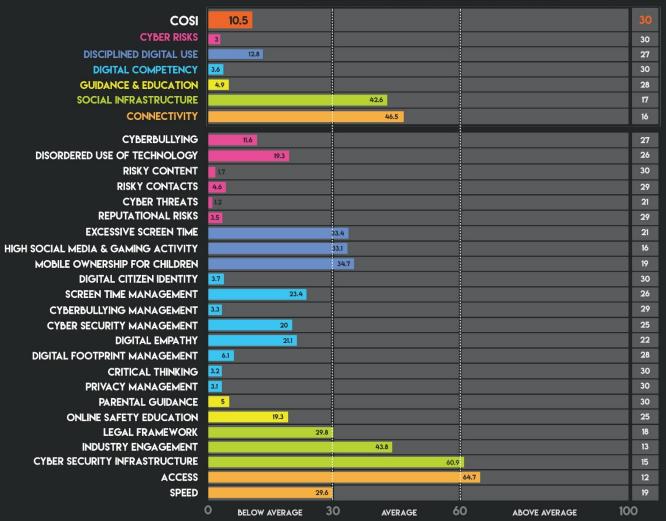
This was classified as a below average performance

## Cyber Risks (30<sup>th</sup>) in Thailand were particularly concerning

– Scores for Cyberbullying (27<sup>th</sup>), Risky Contacts (29<sup>th</sup>), and Reputational Risks (29<sup>th</sup>) must be addressed

## Digital Competency (30<sup>th</sup>) must also be improved

– Digital Citizen Identity (30<sup>th</sup>), Cyberbullying Management (29<sup>th</sup>), Critical Thinking (30<sup>th</sup>), and Privacy Management (30<sup>th</sup>) should be seen as priorities for action





### **TURKEY**

### Turkey ranked 8<sup>th</sup> out of 30 with an overall COSI score of 55.8

This was classified as an average performance

#### Low score for Cyber Risks (25th)

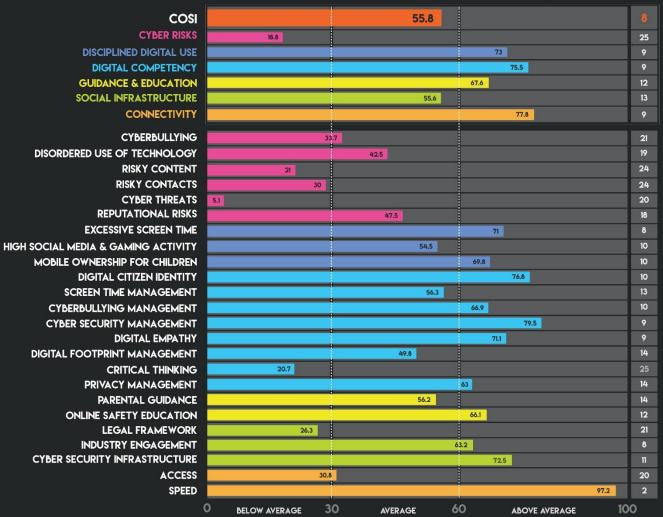
– Performances on Risky Content (24<sup>th</sup>) and Risky Contacts (24<sup>th</sup>) should be improved

#### Mixed performance for Connectivity (9th)

- Strong on Speed (2<sup>nd</sup>), weak on Access (20<sup>th</sup>)









### UNITED KINGDOM

### The United Kingdom ranked 19<sup>th</sup> out of 30 with an overall COSI score of 36.7

This was classified as an average performance

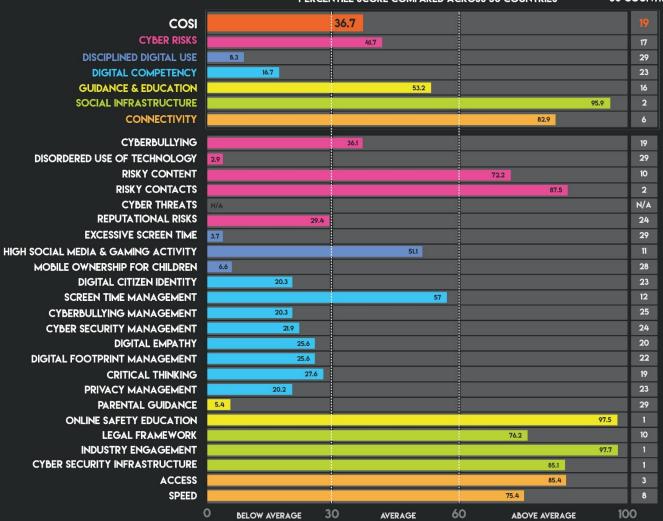
## Disciplined Digital Use (29<sup>th</sup>) must be addressed

– Excessive Screen Time (29<sup>th</sup>) ranked second lowest

#### Scores on Cyber Risks were mixed (17th)

– Disordered Use of Technology (29<sup>th</sup>) a priority for improvement

Highest scores for Online Safety Education (1st), Industry Engagement (1st), and Cyber Security Infrastructure (1st)



### **UNITED STATES**

## The United States ranked 12<sup>th</sup> out of 30 with an overall COSI score of 51

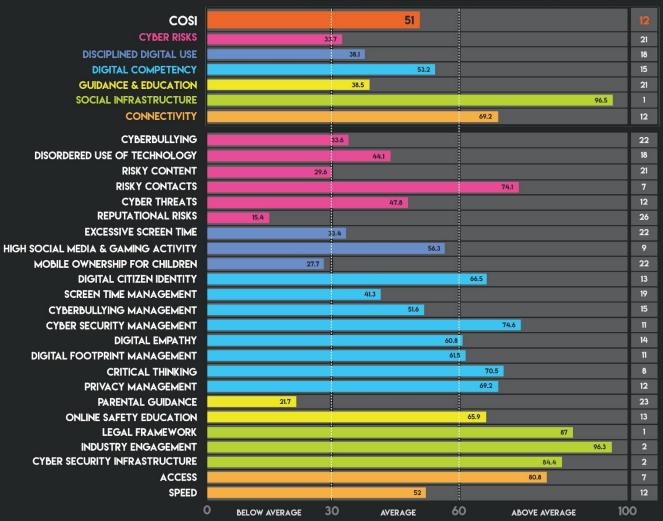
– This was classified as an average performance

## Weakest performances were for Cyber Risks (22<sup>nd</sup>) and Guidance & Education (22<sup>nd</sup>)

– American children were at particular risk of Cyberbullying (22<sup>nd</sup>) and Reputational Risks (26<sup>th</sup>)

## The United States performed well on the pillar of Social Infrastructure (1st)

– Legal Framework (1<sup>st</sup>), Industry Engagement (2<sup>nd</sup>), and Cyber Security Infrastructure (2<sup>nd</sup>) were particularly strong



### **URUGUAY**

### Uruguay ranked 27<sup>th</sup> out of 30 with an overall COSI score of 16.9

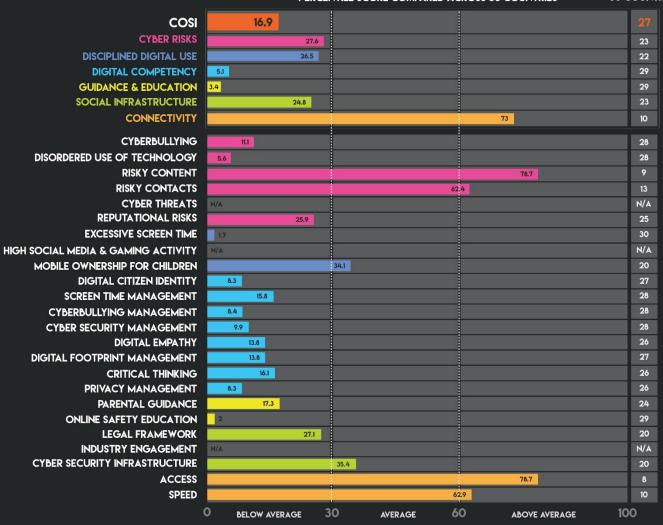
– This was classified as a below average performance

#### Low score for Digital Competency (29th)

– Screen Time Management (28<sup>th</sup>), Cyberbullying Management (28<sup>th</sup>), and Cyber Security Management (28<sup>th</sup>) should be priorities for improvement

### Guidance & Education (29<sup>th</sup>) should be improved

Parental Guidance (24<sup>th</sup>) and Online Safety
 Education (29<sup>th</sup>) both priorities



### **VIETNAM**

## Vietnam ranked 28<sup>th</sup> out of 30 with an overall COSI score of 12.7

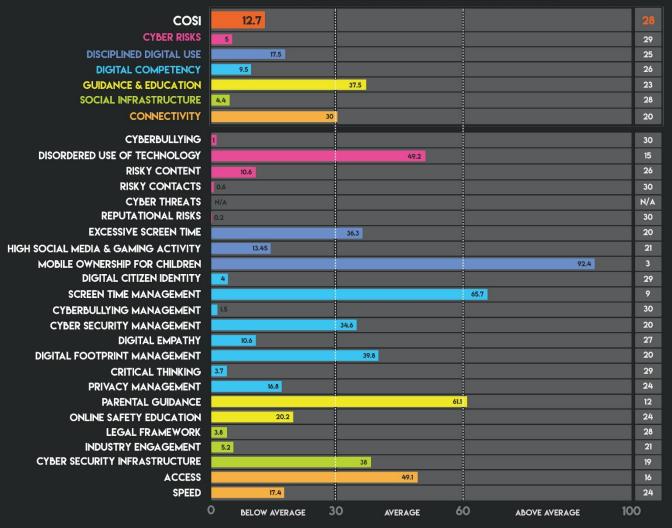
This was classified as a below average performance

#### Low score for Cyber Risks (29th)

– Risky Contacts (30<sup>th</sup>), Cyber Threats (28<sup>th</sup>), and Reputational Risks (30<sup>th</sup>) should be priorities for improvement

## A positive mitigation of risks is found in low Mobile Ownership for Children (4th)

– This can prevent Disordered use of Technology (14<sup>th</sup>)



### **RESEARCH METHODS**

### THE INDEX DEVELOPMENT

This section describes the measurement, scoring, and interpretation information for the 6 pillars and the 24 areas of the COSI. The overall COSI score was based on the average of the scores for the 6 pillars and was scored so that higher values indicate better online safety for children.

### **PILLAR 1: CYBER RISKS**

The Cyber Risks pillar measures the extent to which children are exposed to six different kinds of cyber risks: cyberbullying, disordered use of technology, risky content, risky contacts, cyber threats, and reputational risks. Scores for each area were developed based on how frequently children experienced those risks. The pillar score was created by averaging scores for all six areas. Before averaging, each area score was reversed, so that higher scores for the six areas indicate lower exposure to cyber risks. Likewise, higher scores for the Cyber Risks pillar indicates lower exposure to cyber risks.

### AREA 1: CYBERBULLYING

Cyberbullying is the process of repeatedly and intentionally harassing, mistreating, or making fun of another person online or while using cell phones or other electronic devices (Patchin, 2019). The cyberbullying score measures the following two risky behaviors: (1) cyberbullying, or whether one has cyberbullied other people, and (2) cyber-victimization, or whether one has been cyberbullied by other people.

#### **INSTRUMENTS**

The Cyberbullying Questionnaire (Ang & Goh, 2010) is a set of 9 questions designed to measure cyber-bullying. Respondents are asked if they have been involved in various types of cyberbullying while they were online in the past year. Respondents indicate the frequency of each type of cyberbullying on a 5-point scale (1 = Never, 2 = Once or twice this year, 3 = A few times this year, 4 = About one time every week, 5 = About a few times every week). Example items include: "I made fun of someone by sending/posting stories, jokes or pictures about him/her." and "I kept on sending rude or insulting messages to someone."

The same nine questions were adapted to measure whether the respondent had been cyber-bullied in the past year. Example items include: "Someone made fun of me by sending/posting stories, jokes or pictures about me." and "Someone kept sending me rude or insulting messages."

#### SCORE DEVELOPMENT

The cyberbullying score is designed to capture how many children are affected by cyberbullying through being cyber victimized or engaging in cyberbullying at least once as well as the severity of children's involvement with cyberbullying and cyber-victimization.

The score was developed by aggregating the following three indicators:

INDICATOR	SCORING
The frequency of children's involvement with 9 types of cyberbullying activities.	The average of responses to 9 questions.
The frequency of children's involvement with 9 types of cyber-victimization activities	The average of responses to 9 questions.
The percentage of children affected by cyberbullying.	The percentage of children who were involved in at least one cyber-victimization activity or one cyberbullying activity.

Table 1: Score indicators for Cyberbullying

All three indicators were standardized and reversed, then combined using a weighted average and re-scaled to range from 0 to 100. Higher scores indicate lower cyberbullying.

### **AREA 2: DISORDERED USE OF TECHNOLOGY**

The disordered use of technology score is based on disordered use of video games or social media, as defined by using them in such a way which causes significant dysfunction in a person's life. These categories are defined below.

#### INSTRUMENTS FOR GAMING DISORDER

Gaming Disorder (also known as Internet Gaming Disorder) occurs when a person loses control over video game playing and experiences significant problems because of their persistent gaming behaviors (Lemmens, Valkenburg, & Gentile, 2015). The Diagnostic and

Statistical Manual of Mental Disorders, Fifth Edition (DSM-5) included Internet Gaming Disorder as a condition warranting further research in 2013. More recently, the World Health Organization included Gaming Disorder in the 11th edition of the International Classification of Diseases (ICD-11). Gaming Disorder is currently viewed as a behavioral addiction like gambling disorder and it can occur with both online and offline video games (Gentile et al., 2017).

The items of this measure have been adapted from Lemmens, Valkenberg, and Gentile's (2015) scale used to measure Internet Gaming Disorder. There were a total of 11 questions based on eight of the nine symptoms proposed in the DSM-5. Participants described how frequently they had experienced each symptom in the last year using a 4-point response scale (0 = Don't know, 0 = No, 0.5 = Sometimes, 1 = Yes). Example items include: "Have you felt you could not stop playing video games?" and "Have you experienced serious conflicts with you family or friends because of gaming?"

#### INSTRUMENTS FOR SOCIAL MEDIA DISORDER

Although Social Media Disorder is not yet recognized by the Diagnostic and Statistical Manual of Mental Disorders (DSM) or the International Classification of Diseases (ICD), there is growing evidence that people can also lose control over their social media use, leading to significant problems (van den Eijnden, Lemmens, & Valkenburg, 2016). Thus, Social Media Disorder has been studied as a condition similar to Gaming Disorder.

The measure of Gaming Disorder described above was adapted to measure Social Media Disorder. There were a total of 10 questions based on seven unique symptoms. Participants described how frequently they had experienced each symptom in the last year using a 4-point response scale (0 = Don't know, 0 = No, 0.5 = Sometimes, 1 = Yes). Example items include: "Have you felt you could not stop using social media and chatting apps?" and "Have you experienced serious conflicts with your family or friends because of using social media and chatting apps?"

#### **SCORE DEVELOPMENT**

The disordered use of technology score was designed to capture technology use that is likely to interfere with the rest of a child's life. The DSM-5 suggests that experiencing 5 out of 9 symptoms of Gaming Disorder within a year is sufficient for a diagnosis (Lemmens, Valkenburg, & Gentile, 2015). We assessed 8 unique symptoms of Gaming Disorder and classified children as at risk for Gaming Disorder if they experienced at least half of the symptoms we assessed. Because Social Media Disorder has not been researched as thoroughly as Gaming Disorder, we adopted a conservative threshold for classifying children as at risk for Social Media Disorder experiencing at least 4.5 out of 7 unique symptoms. In

addition to considering the number of children at risk for disordered use of technology, this score also considers the severity of the symptoms associated with disordered use.

The score for this area was developed by aggregating four indicators:

INDICATOR	SCORING
The severity of Gaming Disorder symptoms.	The average of the responses to 11 symptom questions.
The percentage of children at risk for Gaming Disorder.	The percentage of children who experience 4 out of 8 symptoms.
The severity of Social Media Disorder symptoms.	The average of the responses to 10 symptom questions.
The percentage of children at risk for Social Media Disorder.	The percentage of children who experience 4.5 out of 7 symptoms.

Table 2: Score indicators for Disordered Use of Technology

All indicators were standardized and reversed, then combined using a weighted average and re-scaled to range from 0 to 100. Higher scores indicate less disordered use of technology.

### **AREA 3: RISKY CONTENT**

The risky content score is based on exposure to violent and sexual content. Violent content exposure is based on how frequently children play games or watch TV shows, YouTube series, or movies that involve people shooting at, hurting, or killing each other. Sexual content exposure is based on how frequently 8-12 year olds encounter adult content online or how frequently 13-19 year olds receive unwanted sexual content or requests.

We identified exposure to violent and sexual content as risky based on research showing harmful effects. For example, exposure to violent media (such as TV shows and video games) increases the likelihood of aggressive thoughts, feelings, and behaviors and also desensitizes people, leading to less negative reactions to violence (Anderson et al., 2003; Anderson et al., 2010). Violent media exposure also reduces prosocial (or helpful) behavior.

#### INSTRUMENTS FOR EXPOSURE TO VIOLENT CONTENT

Exposure to violent content was assessed with an adaptation of the General Media Habits Questionnaire (Anderson, Gentile, & Buckley, 2007; Gentile, Lynch, Linder, & Walsh, 2004). Participants reported two of their favourite TV shows, YouTube video series, or movies, and two of their favourite video games. Then, for each, they rated how often they watched or

played (1 = Never, 2 = Hardly, 3 = Sometimes, 4 = Often, 5 = Always). They also rated how violent each show or game was (e.g., "How often do characters try to shoot or hurt each other in this show?") using the same 5-point response scale. This approach has been found to be valid in international samples (e.g., Busching et al., 2015).

#### INSTRUMENTS FOR EXPOSURE TO SEXUAL CONTENT (AGES 8-12)

Exposure to sexual content for children aged 8-12 was assessed with survey items. One item assessed passive exposure: "Have you come across sexual content online (like inappropriate photos or videos only for adults)?" A 4-point scale was used (0 = Never, 1 = Seldom, 2 = Sometimes, 3 = Often, 4 = Always). Another item assessed active exposure, based on whether children had done four behaviors (e.g., "Searched for adult topics" or "Lied about age to access adult website"). Scores were based on the number of behaviors selected.

#### INSTRUMENTS FOR EXPOSURE TO SEXUAL CONTENT (AGES 13-19)

Exposure to sexual content for adolescents aged 13-19 was assessed by asking about how many of 6 different unwanted sexual experiences had occurred online in the past year (e.g., "I received unwanted sexual messages or images" or "I received an unwelcome request for sexual favours"). Scores were based on the number of experiences selected.

#### **SCORE DEVELOPMENT**

The score for the Risky Content area was designed to consider the prevalence of exposure to violent and sexual content as well as the severity of that exposure. The scoring for severity of exposure to violent content weighted how violent each show or game was by the frequency of engagement with that media so that the highest scores (before reversing) indicated frequent engagement with violent media and the lowest scores (before reversing) indicated infrequent engagement with nonviolent media. Similarly, we took a conservative approach to classifying children as exposed to violent media--only doing so when they frequently engaged with media that were highly violent. For severity of exposure to sexual media content, scoring differed for children (aged 8-12) and adolescents (aged 13-19). For children, active exposure to sexual content was weighted more heavily than passive exposure to sexual content, because active exposure was within the child's control rather than being incidental. For adolescents, all sexual content experiences were unwanted and were weighted equally. We also took a conservative approach to classifying children and adolescents as exposed to sexual media--only doing so when they had experienced roughly half of the types of sexual media content. Higher risky content scores indicate greater exposure to risky content.

The score for this area was developed by aggregating four indicators:

INDICATOR	SCORING
The percentage of children exposed to violent media content.	The percentage of children who reported high exposure (watching or playing "often" or "always") to three out of four shows or games in which characters were frequently violent (also rated as "often" or "always").
The severity of exposure to violent media content.	How violent the child's favorite media were, weighted by how frequently they engaged with those media.
The percentage of children and adolescents exposed to sexual media content.	The percentage of children and adolescents who scored above 0.5 on the severity of exposure to sexual media content (described below). This roughly corresponds to experiencing more than half of the sexual media situations.
The severity of exposure to sexual media content.	This was calculated differently for children (aged 8-12) and adolescents (aged 13-19).
	For children, scores were based on passive and active exposure. The response to the passive exposure question was divided by four to put this on a 0-1 scale. The number of active exposure items the child experienced were summed, then divided by 4 to put this on a 0-1 scale. The measures of passive and active exposure were then added together after multiplying passive exposure by 0.33 and multiplying active exposure by 0.67 (to weigh active exposure more heavily).
	For adolescents, scores were calculated by summing the number of sexual content situations the adolescent had experienced and dividing by 6 to put this on a 0-1 scale.

Table 3: Score indicators for Risky Content

All indicators were standardized and reversed, then combined using a weighted average and re-scaled to range from 0 to 100. Higher scores indicate lower exposure to risky content.

### **AREA 4: RISKY CONTACTS**

The risky contacts score is based on chatting with strangers online or meeting up with someone in real life whom you met online for children (aged 8-12), and inappropriate contact for children (aged 8-12) and unwanted sexual contact for adolescents (aged 13-19).

We defined this score differently for children and adolescents because different behaviors are riskier (or simply more relevant) for different age groups. Chatting with strangers online, meeting them in real life, or discussing inappropriate topics with them is especially risky for children, who may not be aware of the dangers that may be present in such interactions. Similarly, adolescents are more likely than children to be exposed to unwanted sexual contact or attention online, making those behaviors more relevant to this age group.

#### **INSTRUMENTS FOR RISKY CONTACT FOR CHILDREN (AGES 8-12)**

Risky contact for children was based on three questions. The first two assessed chatting with strangers ("Have you chatted with people you have never met offline?") or meeting up with strangers ("Have you met someone in real life who you only knew online?"), using a 2-point response scale (0 = No, 1 = Yes). Another question assessed how many of three inappropriate contact behaviors children had experienced online (e.g., "Sent someone adult images" or "Received any adult images from someone"). Scores were based on the number of behaviors selected.

### INSTRUMENTS FOR RISKY CONTACT FOR ADOLESCENTS (AGES 13-19)

Risky contact for adolescents was based on how many of six unwanted sexual contact experiences the adolescent had experienced online in the past year. Example experiences include: "I received an unwelcome request to send an intimate image of myself or others" and "Someone demanded that I send them sexual images and threatened to distribute my person information if/when I refused." Scores were based on the number of experiences selected.

#### SCORE DEVELOPMENT

The score for the risky contacts area was designed to consider the number of children and adolescents exposed to risky contacts as well as the severity of that exposure. The severity scores capture the number of risky contact situations that the child or adolescent has experienced, and the percentage scores capture the prevalence of experiencing risky contacts past a minimum threshold.

The score for this area was developed by aggregating four indicators:

INDICATOR	SCORING
The severity of risky contacts.	This was calculated differently for children (aged 8-12) and adolescents (aged 13-19).
	For children, a contact with strangers score was calculated by averaging the number of "yes" responses and a sexual contact score was calculated by averaging the number of sexual contact behaviors the child had experienced (with each scored as 1 if experienced). These two numbers were then averaged, creating a measure that ranged from 0-1.
	For adolescents, an unwanted sexual contact score was calculated by averaging the number of unwanted sexual contact experiences the adolescent had (with each scored as 1 if experienced). This created a measure that ranged from 0-1.
The percentage of children and adolescents experiencing at least one risky contact.	For children, the percentage of children who experienced at least one type of inappropriate contact or offline meeting.
	For adolescents, the percentage was based on the number of adolescents who experienced at least one type of unwanted sexual contact.

Table 4: Score indicators for Risky Contacts

All indicators were standardized and reversed, then combined using a weighted average and re-scaled to range from 0 to 100. Higher scores indicate lower exposure to risky contacts.

### **AREA 5: CYBER THREATS**

The cyber threats score is based on dangers encountered online such as computer viruses, unwanted location tracking, and identity theft.

#### INSTRUMENTS FOR CYBER THREATS

Exposure to cyber threats was measured by asking respondents to select how many of five cyber threats had been experienced online in the past year. Examples of cyber threats include "I lost money by being cheated on the internet" and "The device (e.g., phone, tablet, computer) I use got infected with a virus or spyware." Scores were based on the number of cyber threats experienced.

#### SCORE DEVELOPMENT

The cyber threats score was designed to capture the number of children and adolescents who have experienced cyber threats as well as the percentage of cyber threats they have experienced. We selected a low threshold to assess the prevalence of cyber threats because we believe that experiencing even one is too many.

The score for this area was developed by aggregating two indicators:

INDICATOR	SCORING
The number of cyber threats experienced.	The average of the number of cyber threats experienced (with each experienced being counted as 1).
The percentage of children and adolescents who experienced at least one cyber threat.	The percentage who scored > 0 on the average described above.

Table 5: Score indicators for Cyber Threats

All indicators were standardized and reversed, then combined using a weighted average and re-scaled to range from 0 to 100. Higher scores indicate lower exposure to cyber threats.

### **AREA 6: REPUTATIONAL RISKS**

The reputational risks score is based on having one's reputation harmed by online behaviors or actively harming the reputation of others through one's own online behavior.

This score focuses on aspects of the digital footprints created by children and adolescents, and how the traces that they leave behind online may bring harm to their own reputation or the reputation of others.

#### INSTRUMENTS FOR EXPERIENCING RISKS TO OWN REPUTATION

Experiencing risks to one's own reputation was assessed with five survey items asking about how frequently such risks were experienced using a 5-point response scale (1 = Never, 2 = Once or twice this year, 3 = A few times this year, 4 = About one time every week, 5 = About a few times every week). Example items include: "Someone spread rumours or gossip about me online" and "Someone made fun of me by sending/posting stories, jokes, or pictures about me."

#### INSTRUMENTS FOR RISKING THE REPUTATION OF OTHERS

Risking the reputation of others was assessed with five survey items asking about how frequently the respondent had engaged in behaviors that could harm the reputation of others. The same 5-point response scale was used here. Example items include: "I sent or posted cruel and untrue things about someone" and "I spread rumours or gossip about someone online."

#### SCORE DEVELOPMENT

The reputational risks score was designed to capture the number of children and adolescents affected by reputational risks (the percentages), as well as the frequency of involvement in experiencing or causing reputational risks (the frequency scores). Our percentages focused on the number of children and adolescents who have experienced or caused reputational risks at least once because we believe that even one of these experiences can have serious consequences.

The score for this area was developed by aggregating four indicators:

INDICATOR	SCORING
The frequency of children and adolescents experiencing risks to their own reputation.	The average of responses to 5 items.
The percentage of children and adolescents who have experienced risks to their own reputation at least once.	, ,
The frequency of children and adolescents causing reputational risk to others.	The average of responses to 5 items.

The percentage of children and adolescents involved in causing reputational risk to others at least once.

The percentage who reported at least one activity related to reputational risks.

Table 6: Score indicators for Reputational Risks

All indicators were standardized and reversed, then combined using a weighted average and re-scaled to range from 0 to 100. Higher scores indicate lower reputational risk.

### **PILLAR 2: DISCIPLINED DIGITAL USE**

The Disciplined Digital Use pillar measures the prevalence of excessive screen time, high social media and gaming activity, and mobile ownership for children (aged 8-12). Scores for each area were developed based on the percentage of children passing thresholds described in the following sections. The pillar score was created by averaging the scores for all three areas. Before averaging, each area score was reversed, so that higher scores for the Pillar and for each area indicate more disciplined digital use.

### **AREA 7: EXCESSIVE SCREEN TIME**

The excessive screen time score is based on how much time (in terms of hours) a person spends in front of any screen for entertainment use (e.g., television, smartphones, game consoles, computers).

#### INSTRUMENTS FOR TOTAL SCREEN TIME

The measurement of total screen time was adapted from the General Media Habits Questionnaire (Anderson et al., 2007; Gentile et al., 2004). Respondents were asked to report how many hours they spent (1) watching online videos, TV shows, and movies, (2) playing video games, and (3) using social media or chatting apps. The time reports were made separately for weekdays and weekend days and were also split into different blocks of time: Midnight to 6:00 am, 6:00 am to Noon, Noon to 6:00 pm, and 6:00 pm to Midnight.

#### SCORE DEVELOPMENT

For weekly screen time, 40 hours per week was selected as the threshold for high weekly screen time because spending the equivalent of a full-time job on screen media for entertainment is likely to disrupt a child's ability to participate in other important activities. Note that this is a significantly higher threshold than has been recommended by groups such as the American Academy of Pediatrics, who have recommended no more than 2 hours a day (14 hours per week) of screen entertainment.

The score for this area was developed based on one indicator:

INDICATOR	SCORING
The percentage of children with high weekly screen time.	Those with >= 40 hours per week of screen time, after aggregating responses to weekly watching, playing, and use of social media.

Table 7: Score indicators for Excessive Screen Time

This indicator was standardized and reversed, then re-scaled to range from 0 to 100. Higher scores indicate a lower prevalence of high weekly screen time (suggesting more disciplined use).

#### AREA 8: HIGH SOCIAL MEDIA AND GAMING ACTIVITY

The high social media and gaming activity score is based on the frequency of engagement with social media and video gaming.

#### INSTRUMENTS FOR SOCIAL MEDIA AND GAMING ACTIVITY

Social media and gaming activity were assessed with several different types of survey items. First, respondents reported how frequently they engaged in five different social media activities (e.g., "Posted a comment online" or "Sent an email or chat message through phone app (e.g., Kakao, WhatsApp, WeChat)") and in one type of gaming activity ("Played a video game that plays with other people (e.g., Minecraft, World of Warcraft)"). All of these items used a 5-point response scale (1 = Never, 2 = Seldom, 3 = Sometimes, 4 = Often, 5 = All the time). Respondents also reported how many friends they have on their selected social media platform (< 50, 51-100, 101-250, 250-500, 501-750, 750-1000, > 1000) and how many times a day they check for messages on social media (0-5, 5-10, 10-50, 50+).

#### SCORE DEVELOPMENT

We classified children as highly engaged with social media and gaming activities based on their consistent use of the highest regions of response scales. Such high engagement is likely to disrupt a child's ability to participate in other important activities.

The score for this area was developed based on one indicator:

INDICATOR	SCORING
The percentage of children with high social	The percentage of children meeting the
media and gaming activity.	following criteria:

- Responded with "often" or "all the time" to all 5 social media activity items.
- Have 250+ friends on social media.
- Check for messages on social media more than 10 times per day.
- Play video games with others "often" or "all the time."

Table 8: Score indicators for High Social Media and Gaming Activity

This indicator was standardized and reversed, then re-scaled to range from 0 to 100. Higher scores indicate a lower prevalence of high social media and gaming activity (suggesting more disciplined use).

### AREA 9: MOBILE OWNERSHIP FOR CHILDREN

This area assesses how many children (aged 8-12) own a mobile phone or smartphone with internet access.

#### INSTRUMENTS FOR MOBILE OWNERSHIP FOR CHILDREN

Mobile ownership for children was assessed with a single survey item, which asked respondents to select which devices they usually use to access the internet. Among these options was "My mobile phone / smartphone."

#### SCORE DEVELOPMENT

We focused on the mobile ownership of young children (aged 8-12) rather than older children (aged 13-19) because young children are likely to struggle more with regulating their own internet use if they own a mobile phone which allows for constant connection.

The score for this area was developed based on one indicator:

INDICATOR	SCORING
	The percentage of children who reported using their own mobile phone or smartphone to access the internet.

Table 9: Score indicators for Mobile Ownership for Children

This indicator was standardized and reversed, then re-scaled to range from 0 to 100. Higher scores indicate a lower prevalence of mobile ownership among children (suggesting more disciplined use).

#### PILLAR 3: DIGITAL COMPETENCY

The Digital Competency pillar is designed to assess the level of digital competencies among children that allow them to mitigate cyber risks and maximize the positive use of technology. It is based on eight DQ digital citizenship competencies that allow children to use digital technology and media in safe, responsible, and ethical ways (DQ Institute, 2019). These competencies are defined in the following sections. The pillar score was created by averaging the scores for all eight competencies (or areas). Higher scores for the Pillar and for each area indicate greater *digital competency*.



Figure 15: Eight competencies of DQ Digital Citizenship

This collective set of digital citizenship competencies enable children to not only deal with the challenges and demands of their digital lives, but also to take responsibility in their digital communities and create value in the digital economy.

The competencies help enhance the resilience of individuals and organizations, the sustainability of digital environments with trust and transparency among stakeholders and, lastly, ignite the growth engines needed to catalyze new heights of digital innovation. Ultimately, having citizens with high competency will heighten the well-being of individuals and communities, ensure the security of our societies, and enhance the economic benefits of nations.

This pillar score was developed from the DQ composite in the DQWorld.net algorithm which is the standardized value of the average score of all eight areas with a mean of 100 and a standard deviation of 15. When a sample was from other data sources, it was estimated based

on multiple regression prediction models based on the overlapping questions between DQ World and other data sources. After the DQ composite score was derived, it was then transformed into a percentile score (ranging from 0-100) for aggregation across six pillars. Higher scores for the pillar and for each area indicate greater digital competency.

## **AREA 10: DIGITAL CITIZEN IDENTITY**

The digital citizen identity score refers to the ability to build and manage a healthy identity as a digital citizen with integrity.

## **INSTRUMENTS**

Survey-based measures were used to assess the following:

COMPETENCY	KNOWLEDGE	SKILLS	ATTITUDES/BEHAVIORS/ VALUES
Digital Citizen Identity	Knowledge of digital media and technology	Skills to build ones' digital identity to be consistent with their offline identity  Global citizenship	Congruence between online and offline behaviors Self-efficacy

Table 10: Assessment criteria for Digital Citizen Identity

## SCORE DEVELOPMENT

Indicators were aggregated based on weighted arithmetic averaging after transformation of the raw scores. This composite score was then standardized with a global average of 100 and a standard deviation of 15. For the purpose of the development of the COSI, the aggregated score for country was re-scaled into 0-100 based on percentile of score.

We weighted online identity management and global citizenship equally because we believe that both are equally important for maintaining a healthy identity as a digital citizen. Higher scores indicate a stronger digital citizen identity.

# **AREA 11: SCREEN TIME MANAGEMENT**

The screen time management score refers to the ability to manage and balance one's online and offline lives by exercising self-control to manage total screen time and engagement with digital media and devices.

## **INSTRUMENTS**

Survey-based measures were used to assess the following:

COMPETENCY	KNOWLEDGE	SKILLS	ATTITUDES/BEHAVIORS/ VALUES
Screen Time Management	Knowledge about screen time, multi- tasking, and their impact on development	Time management skills	Screen time and digital media usage habits Self-regulation

Table 11: Assessment criteria for Screen Time Management

#### **SCORE DEVELOPMENT**

The scores of these indicators were aggregated based on weighted arithmetic averaging after transformation of the raw scores. This new score was then standardized with a global average of 100 and a standard deviation of 15. For the purpose of the development of the COSI, the aggregated score for country was re-scaled into 0-100 based on percentile of score.

We weighted the measures nearly equally but chose to place greater emphasis on children's level of disordered gaming and self-regulation of internet activities because these areas are more likely than the other two to interfere with (or support) a child's ability to manage their own screen time. Higher scores indicate better screen time management.

# **AREA 12: CYBERBULLYING MANAGEMENT**

The cyberbullying management score refers to the ability to identify cases of cyberbullying and handle them wisely.

## **INSTRUMENTS**

COMPETENCY	KNOWLEDGE	SKILLS	ATTITUDES/BEHAVIORS/ VALUES
Cyberbullying Management	Knowledge about cyberbullying and its impact on	Skills to regulate emotions  Skills to deal with	Cyberbullying involvement behaviors
	relationships	cyberbullying incidences	Attitude toward cyberbullying acts

Table 12: Assessment criteria for Cyberbullying Management

The scores of these indicators were aggregated based on weighted arithmetic averaging after transformation of the raw scores. This new score was then standardized with a global average of 100 and a standard deviation of 15. For the purpose of the development of the COSI, the aggregated score for country was re-scaled into 0-100 based on percentile of score.

We weighted measures so that cyberbullying involvement (representing poor management abilities) and cyberbullying management (representing good management abilities) were represented equally. Within cyberbullying involvement, past behaviors were weighted more strongly than attitudes because actually engaging in cyberbullying is more serious than simply having a positive attitude towards it. Within cyberbullying management, a child's approach to dealing with being cyberbullied and knowledge about cyberbullying were weighted approximately equally. Higher scores indicate better management of cyberbullying (and low involvement in cyberbullying engagement).

# **AREA 13: CYBER-SECURITY MANAGEMENT**

The cyber-security management score refers to the ability to protect one's data by creating strong passwords and handling various cyber-attacks.

#### **INSTRUMENTS**

COMPETENCY	KNOWLEDGE	SKILLS	ATTITUDES/BEHAVIORS/ VALUES
Cybersecurity Management	Cybersecurity knowledge	Skills to make strong passwords and keep them safely	Cybersecurity behaviors  Cybersecurity attitudes
		Skills to detect and deal with cyber threats (e.g., Scams/spam/phishing)	

Table 13: Assessment criteria for Cyber-Security Management

The scores of these indicators were aggregated based on weighted arithmetic averaging after transformation of the raw scores. This new score was then standardized with a global average of 100 and a standard deviation of 15. For the purpose of the development of the COSI, the aggregated score for country was re-scaled into 0-100 based on percentile of score.

We weighted cyber threat management skills, and especially knowledge about scams, phishing, and mobile security, more heavily than password management skills because cyber threats involve others actively seeking to exploit children and because knowledge about these threats allows children to be wary of them. Higher scores indicate better cyber security management.

## **AREA 14: DIGITAL EMPATHY**

The digital empathy score refers to the ability to show empathy toward other people online, respecting their needs and feelings.

## **INSTRUMENTS**

COMPETENCY	KNOWLEDGE	SKILLS	ATTITUDE/BEHAVIORS/ VALUES
Digital Empathy	Knowledge of empathy  Mechanisms of online trolls	Skills to communicate online in non-judgmental and empathetic ways	Empathy, which assesses the extent to which a child can empathize with another person's emotions

Table 14: Assessment criteria for Digital Empathy

The scores of these indicators were aggregated based on weighted arithmetic averaging after transformation of the raw scores. This new score was then standardized with a global average of 100 and a standard deviation of 15. For the purpose of the development of the COSI, the aggregated score for country was re-scaled into 0-100 based on percentile of score.

Empathy was weighted more heavily than knowledge about empathy because we believe the ability to empathize with others is far more important than simply understanding the nature of empathy. Higher scores indicate greater digital empathy.

# **AREA 15: DIGITAL FOOTPRINT MANAGEMENT**

The digital footprint management score refers to the ability to understand the nature of digital footprints and their real-life consequences as well as the ability to manage them responsibly.

## **INSTRUMENTS**

COMPETENCY	KNOWLEDGE	SKILLS	ATTITUDE/BEHAVIORS/ VALUES
Digital Footprint Management	Knowledge of digital footprints	Skills to control digital	Digital footprint behaviors
ivianagement	and reputations	footprints and reputations	Digital footprint attitudes

Table 15: Assessment criteria for Digital Footprint Management

The scores of these indicators were aggregated based on weighted arithmetic averaging after transformation of the raw scores. This new score was then standardized with a global average of 100 and a standard deviation of 15. For the purpose of the development of the COSI, the aggregated score for country was re-scaled into 0-100 based on percentile of score.

We weighted knowledge about digital footprints most strongly because understanding the importance of keeping track of one's digital footprint is a crucial component for successful management. In contrast, we placed less emphasis on digital footprint awareness because awareness of which activities leave digital traces alone is insufficient for successful management--it must be paired with the skills to do so. Higher scores indicate better digital footprint management.

## **AREA 16: CRITICAL THINKING**

The critical thinking score refers to the ability to distinguish between true and false information, good and harmful content, and trustworthy and questionable contacts online.

## **INSTRUMENTS**

COMPETENCY	KNOWLEDGE	SKILLS	ATTITUDE/BEHAVIORS/ VALUES
Critical Thinking	Media and information literacy knowledge	Skills to detect false information and news	Media usage behavior and attitudes
	knowleage	Skills to block unwanted contacts	Evaluation of online information
		Skills to block violent and inappropriate contents	Usage of violent and/or sexual online content
			Chatting and meeting with online strangers

Table 16: Assessment criteria for Critical Thinking

The scores of these indicators were aggregated based on weighted arithmetic averaging after transformation of the raw scores. This new score was then standardized with a global average of 100 and a standard deviation of 15. For the purpose of the development of the COSI, the aggregated score for country was re-scaled into 0-100 based on percentile of score.

We chose to weight the content evaluation and management, information evaluation, and online contact evaluation and management nearly equally because we believe they are similarly important for successful critical thinking in digital contexts. Higher scores indicate better critical thinking.

## **AREA 17: PRIVACY MANAGEMENT**

The privacy management score refers to the ability to handle all personal information shared online with discretion to protect one's own privacy and the privacy of others.

## **INSTRUMENTS**

Survey-based measures were used to assess the following:

COMPETENCY	KNOWLEDGE	SKILLS	ATTITUDE/BEHAVIORS/ VALUES
Privacy Management	Knowledge of personal information and	Skills to protect personal data of themselves and others	Behaviors surrounding personal information sharing
	privacy	Skills to manage privacy	Attitudes toward personal information sharing
		settings on social media	Respect

Table 17: Assessment criteria for Privacy Management

#### SCORE DEVELOPMENT

The scores of these indicators were aggregated based on weighted arithmetic averaging after transformation of the raw scores. This new score was then standardized with a global average of 100 and a standard deviation of 15. For the purpose of the development of the COSI, the aggregated score for country was re-scaled into 0-100 based on percentile of score.

We chose to weigh the protection of others' personal information more strongly than the management of one's own personal information because the former has the potential to affect many people whereas the latter is limited to affecting one person. Higher scores indicate better privacy management.

## PILLAR 4: GUIDANCE AND EDUCATION

Guidance and Education on how to safely and ethically navigate and utilize the internet is important for children to develop digital intelligence. This must come in the form of direct support for children, both from the parents and school. Thus, guidance and education can be defined by the following two aspects: (1) Parental Guidance and (2) Online Safety Education. The score for this pillar was created by averaging scores for these two areas. Higher scores for the pillar and for each area indicate greater better guidance and education.

## **AREA 18: PARENTAL GUIDANCE**

The parental guidance score is based on the extent to which parents monitor and mediate their child's digital media usage. Mediation refers to strategies used by parents to restrict the amount and content of media consumption or to reduce the potential negative effects of media use through active discussion.

#### **INSTRUMENTS**

The measure for parental guidance was adapted from the United Kingdom Children Go Online (Livingstone & Bober, 2004) and European Union Kids Online projects (Livingstone & Haddon, EU Kids Online, 2009). It contains 9 items to check active and restrictive styles of parental mediation. Both styles provide guidance for children as they navigate the digital world. Restrictive mediation involves limiting the use of media (e.g., "Do your parents have set rules about when and how much time you can spend online, play games, and watch videos?") and active mediation involves actively discussing media content (e.g., "My parents explain to me why some websites are good or bad"). All items used a 5-point response scale (1 = Never, 2 = Seldom, 3 = Sometimes, 4 = Often, 5 = All the time).

## SCORE DEVELOPMENT

The parental guidance score was designed to capture both the number of children experiencing high levels of parental mediation (the percentage) and the level at which that parental mediation is experienced.

The score for this area was developed by aggregating two indicators:

INDICATOR	SCORING
The level of parental mediation.	The average of 9 items (after reverse coding, as necessary).

The percentage of children	experiencing	The percentage of children scoring > 3 on
high levels of parental mediation		the average described above.

Table 18: Score indicators for Parental Guidance

All indicators were standardized, then combined using a weighted average and re-scaled to range from 0 to 100. Higher scores indicate more parental mediation (or more guidance).

# **AREA 19: ONLINE SAFETY EDUCATION**

The online safety education score is based on the School Digital Education Index, which measures the level of a child's digital knowledge as learned from school in reference to the usage and safety of digital media.

## **INSTRUMENTS**

The School Digital Education Index consists of two items: "My school teachers teach me about internet safety" and "My school teachers teach me how to use the computer and internet." Both items use a 5-point response scale (1 = Never, 2 = Rarely, 3 = Sometimes, 4 = Regularly, 5 = Many times).

## **SCORE DEVELOPMENT**

The online safety education score was designed to capture both the number of children experiencing frequent online safety education at school (the percentage) and the specific frequency at which such education is experienced.

The score for this area was developed by aggregating two indicators:

INDICATOR	SCORING
The frequency of school online safety education.	The average of 2 items.
The percentage of children experiencing frequent online safety education at school.	

Table 19: Score indicators for Online Safety Education

All indicators were standardized, then combined using a weighted average and re-scaled to range from 0 to 100. Higher scores indicate better education.

## **PILLAR 5: SOCIAL INFRASTRUCTURE**

The Social Infrastructure pillar refers to whether social systems are in place that protect children from cyber risks and promote digital intelligence.

Based on the 2019 Child Online Safety Report developed by the Broadband Commission for Sustainable Development, this pillar emphasizes the following three areas of the social infrastructure to ensure nations to build child online safety.

- 1. Legal Framework
- 2. Cyber Security Infrastructure
- 3. Industry Engagement

The scores for the Social Infrastructure pillar are based on data from the Economist Intelligence Unit (2019). The following sections summarize their methodology used to obtain the scores for these three areas. The three area scores were averaged to obtain the pillar score. Higher scores indicate better social infrastructure.

## **AREA 20: LEGAL FRAMEWORK**

The Legal Framework score refers to whether there is appropriate legislation within countries for promoting the safety of children online. We assessed this with two measures from external sources: the Online Grooming Score, and the Child Sexual Abuse Material (CSAM) Legal Score (Broadband Commission for Sustainable Development, 2019).

## INSTRUMENT FOR THE ONLINE GROOMING SCORE

The Online Grooming Score is taken from the Out of the Shadows Index (2019), a 60-country benchmarking study (Economist Intelligence Unit, 2019). This score considers whether there is legislation designed to protect children from online grooming. Online grooming occurs when an adult uses the internet to trick or coerce a child into sexual activities. Thus, this score evaluates how stakeholders are responding to the scourge of sexual violence against children in 60 countries. The score examines four categories within which responses to sexual violence against children occur: (1) Environment, (2) Legal Framework, (3) Government Commitment and Capacity and (4) Engagement of Industry, Civil Society, and Media.

The Online Grooming Score is the weighted average of four scores (see Table 20). For each score, the index used the findings from a qualitative assessment conducted by the International Centre for Missing and Exploited Children which provided either a yes (100) or no (0) response to whether there is legislation in place for each score type.

INDICATOR	DESCRIPTION
Legislation specific to online grooming	Is there legislation specific to online grooming in the country? (yes/no)
Online grooming with intent to meet the child	Is there legislation against online grooming with intent to meet the child? (yes/no)
Online grooming regardless of intent to meet the child	Is there legislation against online grooming regardless of intent to meet the child? (yes/no)
Showing pornography to a child	Is there legislation against showing pornography to a child? (yes/no)

Table 20: Score indicators for Online Grooming Score from the Out of the Shadows Index

Together, the weighted average of the four scores provide a score from 0 to 100, where 100 indicates the best environment for children (i.e., the best legislation for online grooming and child protection).

## INSTRUMENT FOR THE CHILD SEXUAL ABUSE MATERIAL (CSAM) LEGAL SCORE

Scores on legislation against Child Sexual Abuse Material (CSAM) were taken from the International Centre for Missing and Exploited Children (ICMEC)'s Global CSAM Legislation Review (ICMEC, 2018). The review assessed whether national legislation in 180 countries:

- 1. Exists with specific regard to CSAM;
- 2. Provides a definition of CSAM;
- 3. Criminalizes technology-facilitated CSAM offenses;
- 4. Criminalizes the knowing possession of CSAM, regardless of the intent to distribute;
- 5. Requires Internet Service Providers (ISPs) to report suspected CSAM to law enforcement or some other mandated agency.

The following is a general summary of their results in reference to these 5 criteria. 118 countries had legislation sufficient to combat CSAM offenses (at least four criteria). Of these, 21 countries met all 5 criteria and 97 countries met 4 criteria. There were 16 countries with no legislation specifically addressing CSAM (0 criteria). Of the remaining 62 countries that had legislation addressing CSAM:

- 51 countries did not define CSAM.
- 25 countries did not criminalize technology-facilitated CSAM offenses.
- 38 countries did not criminalize the knowing possession of CSAM, regardless of the intent to distribute.

Taking the results for each country from ICMEC, we scored countries from 0-5, depending on how many of the 5 criteria above were met by national legislation in the country (1 criterion met = score of 1, 2 criteria met = score of 2, and so on). This was then transformed into a score out of 100, where 100 = national legislation for CSAM meets all 5 criteria.

## **SCORE DEVELOPMENT**

We weighted the Online Grooming Score and the CSAM Legal Score equally because the two are similarly important for promoting the safety of children online.

The score for the Legal Framework score was calculated by first standardizing and averaging the Online Grooming Score and the CSAM Legal Score. In order to be combined with other scores, it was re-scaled into 0-100 as a percentile score to serve as the Legal Framework score. Higher scores indicate greater protection for children in existing legal frameworks.

## **AREA 21: CYBER SECURITY INFRASTRUCTURE**

The cyber security infrastructure score refers to the extent to which nations have infrastructure promoting cyber security. Good infrastructure supporting cyber security indicates that nations have the capacity to keep children safe online and suggests that the nation is committed to online safety.

## **INSTRUMENTS**

The Global Cybersecurity Index (GCI; International Telecommunication Union, Global Cybersecurity Index, 2018) was used to assess cyber security infrastructure. GCI is an index that combines 25 scores into one benchmark measure to monitor and compare the level of International Telecommunication Union (ITU) Member States' cybersecurity commitment in relation to five pillars identified by high-level experts and endorsed by ITU's Global Cybersecurity Agenda. These five pillars are: (1) Legal, (2) Technical, (3) Organizational, (4) Capacity Building, and (5) Cooperation.

For each of the pillars, country commitment was assessed through question-based online surveys. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score. Higher GCI scores indicate a higher commitment to cybersecurity, which protects children from cyber-risks.

GCI scores ranged from 0-1. In order to be combined with other scores, it was standardized and re-scaled into 0-100 as a percentile score to serve as the cyber security infrastructure score. Higher scores indicate better cyber security infrastructure which should promote child online safety.

## **AREA 22: INDUSTRY AND CIVIC ENGAGEMENT**

The industry engagement score refers to the extent to which industry and civic sectors are involved in ensuring the safety of children online.

## **INSTRUMENTS**

Scores for this area were based on the Engagement of Industry, Civil Society, and Media score for each country, extracted from the Out of the Shadows Index (2019) (Economist Intelligence Unit, 2019). This score ranges from 0-100 and assesses the propensity for addressing risks to children at the industry and community levels, as well as providing support for victims. It is based on the weighted average of 5 scores, which are themselves based on the weighted average of their respective sub-scores (see the following sections for full information). Higher scores indicate better engagement in protecting children.

## TECHNOLOGY INDUSTRY ENGAGEMENT

This refers to the ability of technology sector stakeholders to institute mechanisms for reporting and collaborating to remove child sexual abuse material illustrates the extent to which actors are responding to the problem of online child sexual abuse and exploitation.

The score is the weighted average of the following sub-scores (with scoring information shown below each description):

- Technology industry reporting mechanisms: Does the country have its own notice and takedown system to allow members of the public to report potentially unlawful child sexual abuse content so that it can be quickly removed? And/or does the country participate as a member of an international notice and takedown system network?
  - 0 = no to either
  - o 1 = yes to one or both
- Response of the mobile telecom industry: Does the leading national (mobile) telecoms association include issues of sexual violence against children in its annual report or code of conduct, or as a clear priority in its scope of work?

- o 0 = no or information is not available / inexplicit
- $\circ$  1 = yes
- Response of the internet industry: Does the leading national internet industry association include issues of sexual violence against children in its annual report or code of conduct, or as a clear priority in its scope of work?
  - o 0 = no or information is not available / inexplicit
  - 0 1 = yes

## TRAVEL AND TOURISM INDUSTRY ENGAGEMENT

This refers to the participation of industry players in the travel and tourism sector illustrates the extent to which it is engaged in efforts to combat violence against children.

The score is the weighted average of the following sub-scores (with scoring information shown below each description):

- Commitment to the Code (headquartered companies): Has any company headquartered in the country signed up to "The Code of Conduct for the Protection of Children from Sexual Exploitation in Travel and Tourism?"
  - 0 = no
  - 0 1 = yes
- Commitment to the Code (operators): Has any company with operations in the country signed up to "The Code of Conduct for the Protection of Children from Sexual Exploitation in Travel and Tourism?"
  - 0 = n0
  - o 1 = yes
- Response of travel and tourism industry: Does the national travel and tourism industry association include issues of sexual violence against children in its annual report or code of conduct, or as a clear priority in its scope of work?
  - o 0 = no or information is not available / inexplicit
  - 0 1 = yes

## FRONTLINE SUPPORT WORKERS

This refers to the availability of professional support and guidance to support workers can facilitate appropriate responses.

The score is the weighted average of the following sub-scores (with scoring information shown below each description):

• Guidelines for teaching professionals: Does a professional body or industry interest group in the country provide guidelines for responding to sexual violence against

children either as a dedicated issue or part of general guidance on responding to sexual violence?

- o 0 = no or information is not available / inexplicit
- o 1 = yes
- Guidelines and protocols for healthcare workers: Does a professional body or industry
  interest group in the country provide guidelines or standard operating procedures for
  responding to sexual violence against children either as a dedicated issue or part of
  general guidance on responding to sexual violence?
  - o 0 = no or information is not available / inexplicit
  - o 1 = yes
- Guidelines for social workers: Does a professional body or industry interest group in the country provide guidelines for responding to sexual violence against children either as a dedicated issue or part of general guidance on responding to sexual violence?
  - o 0 = no or information is not available / inexplicit
  - 0 1 = yes
- Guidelines for psychiatric workers: Does a professional body or industry interest group in the country provide guidelines for responding to sexual violence against children either as a dedicated issue or part of general guidance on responding to sexual violence?
  - o 0 = no or information is not available / inexplicit
  - 0 1 = yes

## CIVIL SOCIETY ENGAGEMENT

Non-governmental organizations (NGOs), foundations, non-profit organizations, community associations and neighbourhood associations are often at the frontline of responding to sexual violence against children, providing education, social welfare and legal services in response to sexual violence against children in the community, and filling critical gaps in service delivery. This index assesses the extent to which civil society is engaged in combating sexual violence against children.

The score is the weighted average of the following sub-scores (with scoring information shown below each description):

- Civil society organization support: Do civil society organizations exist that provide the following support services for victims related to (a) medical support, (b) emergency accommodation and care for victims, (c) therapeutic care, (d) legal aid, and (e) education and awareness raising?
  - 0 = no
  - o 1-5 = yes, with one point awarded for each aspect of the above care available
- Existence of civil society organizations (offenders): Are there civil society organizations (CSOs) in the country that provide preventive or rehabilitative support to offenders?

- o 0 = no, there are no nationally recognized CSO that provide therapeutic services to support offenders
- o 1 = yes, there is at least one nationally recognized CSO that provides therapeutic services to support offenders

## MEDIA INDUSTRY ENGAGEMENT

The response of the media in covering sexual violence can be influential in driving social change and shaping attitudes related to sexual violence against children. This index assesses how involved the media industry is in combating sexual violence against children.

The score is based on the following (with scoring information shown below each description):

- Guidelines for journalists/media: Does a professional body or interest group provide guidelines for reporting on sexual violence against children, either as a dedicated issue or part of general guidance on responding to sexual violence?
  - o 0 = no or information is not available/inexplicit
  - o 1 = yes

#### SCORE DEVELOPMENT

We used the scoring approach developed for the Out of the Shadows Index (Economist Intelligence Unit, 2019) for this score. We standardized the score and re-scaled into 0-100 with a percentile score to allow for aggregation with other scores. Higher scores indicate greater engagement of industry and other sectors in the protection of children.

## **PILLAR 6: CONNECTIVITY**

We believe that every child should have good connectivity to the internet, allowing for useful and empowering internet experiences. Connectivity can be defined by access and speed. These two areas are defined in the following sections. Scores for the Connectivity pillar were created by averaging the two area scores. Higher scores indicate better connectivity.

## **AREA 23: ACCESS**

The access score assesses whether children are able to access the internet through hardwired (e.g., ethernet) or mobile (e.g., Wi-Fi) connectivity (or both).

#### **INSTRUMENT**

The score for the access area is calculated by aggregating the following four indicators:

- 1. Percentage of individuals using the internet
- 2. Number of fixed broadband subscriptions (per 100 habitants)
- 3. Number of mobile cellular subscriptions (per 100 habitants)
- 4. The Mobile Connectivity Index from the Global System for Mobile Communications Association (GSMA)

The first three indicators were derived from the International Telecommunication Union (ITU)'s aggregated metadata which provides this information for many countries (International Telecommunication Union, 2019).

The fourth indicator, GSMA's Mobile Connectivity Index, measures the performance of 165 countries based on the key enablers of mobile internet adoption: Infrastructure, Affordability, Consumer Readiness, and Content and Services (Global System for Mobile Communications, 2019). Countries are scored from 0 to 100 across several scores, with higher scores representing stronger performance in delivering mobile internet connectivity.

## **SCORE DEVELOPMENT**

The score for the access area was created by aggregating the four indicators described above. The four measures were standardized and averaged, and then transformed to a percentile scale ranging from 0-100.

## **AREA 24: SPEED**

The speed score assesses whether children are able to access the internet with sufficient speeds to have a full internet experience. In other words, internet speed (including download and upload speeds) should not stand in the way of children and adolescents fully using the online applications that they consider important.

Download speed refers to "how quickly you can pull data from a server on the internet to your device. Most connections are designed to download much faster than they upload. This is because the majority of online activity, like loading web pages or streaming videos, consists of downloads" (Ookla, 2019).

Meanwhile, upload speed refers to "how quickly you send data from your device to the internet. A fast upload speed is helpful when sending large files via email, or in using videochat to talk to someone else online (since you have to send your video feed to them)" (Ookla, 2019). Both download and upload speeds are measured in megabits per second (Mbps).

## **INSTRUMENT**

We used the mobile upload and download speeds provided by Ookla's SpeedTest® Global Index (Ookla, Speedtest Global Index, 2019). Ookla uses consumer-initiated testing to collect such internet speed data. To be included in its SpeedTest Global Index, countries and regions must have at least 300 unique user results for mobile or fixed broadband to be ranked in either category.

For reference, a good internet speed is at or above 25 Mbps. These speeds will support most online activities, including web browsing, streaming of videos in high-definition quality and playing online games. An internet connection with fast internet speeds of above 100 Mbps are usually preferred for users looking to support numerous devices and/or users simultaneously (Anders, 2019). For upload, connection speeds of 10 Mbps or higher are generally considered fast because they can easily handle the common upload activities of the average user.

#### SCORE DEVELOPMENT

The score for the speed area was created by aggregating two indicators: upload and download speeds. The two indicators were standardized and averaged, then transformed to a percentile scale ranging from 0-100.

We chose to weight both indicators equally because we believe that both are essential to having a meaningful internet experience. Higher scores indicate better speed.

# DATA AND METHODOLOGY

# **DATA COLLECTION**

The data were collected through three different mediums: (1) the online platform DQWorld.net, (2) DQTest.org, and (3) the DQ student survey.

The DQWorld.net is a main online platform to collect children's data. As the children engage in the various "missions" on the platform, they complete surveys and quizzes that reinforce the interactive activities. Each child's responses are tracked in order to measure progress, assess risk, and generate the child's data. The self-reporting survey questions related to social emotional abilities, and responsible cyber attitudes/behaviors are asked along with various interactive activities and quizzes that are asked to test technical and critical reasoning abilities.

The DQTest.org and DQ student surveys were shortened forms of the questions and surveys used on DQWorld.net and were designed to assess similar concepts in less time. All questions in the DQTest.org and the DQ student surveys are available on DQWorld.net. The amount of time required to fill out the DQTest.org and the DQ student surveys was around 60 minutes and the amount of time to complete all activities on DQWorld.net was around 10 hours. No incentives were offered for participation.

All questions from the DQTest.org and DQ student survey were then matched with those from DQWorld.net to allow us to combine the data.

Children were recruited with the aid of teachers and school administrators who were contacted by partners located in each country. The children participated through their schools, either in the classroom or at home on the website where the survey and test were hosted. In some countries, pen and paper surveys were used, with results coded and shared by teachers.

These surveys provided data for many of the scores used in the COSI framework.

# RESEARCH PROCEDURE

The entire process for child participants was conducted through three online platforms, (1) DQWorld.net, (2) DQTest.org, and (3) the DQ student survey, unless the schools chose to conduct the survey in offline. However, in order to start online activities for the children, there were three procedures that were completed prior to initiating the online experience.

1. Invitation to schools: Interested schools were invited for a briefing session to share the aims of the study, what the DQ World programme is about, implementation guidelines and role of teachers and key personnel involved.

- 2. Teachers' briefing and registration: Teachers from the participating schools were informed about the DQWorld online learning experience and the proposed research aims. The teachers were guided to register their children' online accounts on the DQWorld online portal.
- 3. Parental opt-out option: An opt out form was given to parents to inform them of child's participation in study prior to starting where they may choose to withdraw their child from the study.

# SAMPLE SIZE

Across the three online programs, a total of 145,426 children and adolescents (aged 8-19 years old; 51% male) from 30 countries were collected from March 2017 to December 2019.

COUNTRY	TOTAL
Thailand	47,130
Singapore	11,963
Mexico	11,773
Philippines	11,390
Japan	7,638
Australia	6,310
Spain	4,590
Colombia	4,335
Turkey	4,183
Peru	4,137
Nigeria	3,387
Indonesia	3,247
United States	2,896
Hong Kong	2,608
New Zealand	2,394
Ecuador	1,808
India	1,736
South Africa	1,707
Vietnam	1,707
Italy	1,691
Nepal	1,459
Oman	1,148
Malaysia	1,135
Dominican Republic	1,044
Korea	939
Uruguay	864
China	816
Saudi Arabia	594
United Kingdom	416
Egypt	381
Total	145,426

Table 21: Total sample size from each country

## **COMPUTATION OF SCORES**

The COSI score is calculated by successively aggregating concepts at each level of the hierarchy. (For more details, see "The COSI Framework" section of this report.)

The six pillar scores (Cyber Risks, Disciplined Digital Use, Digital Competency, Guidance & Education, and Connectivity) were created based on aggregation of the scores of 24 areas which are each based on multiple indicators.

For example, at the lowest level, each indicator to develop each score of the 24 areas was standardized and each score was developed based on a weighted average of the indicators belonging to each area. It is then transformed to 0-100 values as a percentile score across the countries. This means that all area scores range from 0 (the lowest possible score) to 100 (the highest possible score). These area scores were averaged to create a score for each of the six pillars. The overall COSI score is then created by developing a geometric average of the six pillar scores.

# ADJUSTMENT BASED ON AGE GROUP AND DATA SOURCES

Because we used convenience sampling, the number of participants is not equal across the age groups. Thus, we checked for statistically significant differences between the age groups for our measures. Moreover, we checked for statistically significant difference across three data sources. When statistically significant differences were found, we calculated the measures separately and developed the weighted average based on the sampling size as well as the geographic representation of the sampling of the data sources to better represent the sample to be nationally representative.

# **LIMITATIONS**

Our results should be interpreted with a few limitations in mind. Because this study was conducted as part of the #DQEveryChild initiative, our participants served as a convenience sample and the number of participants from each country varied depending on the extent of the initiative's adoption in that country. Thus, although our results tell us about the online safety of children in 30 different countries, these results may not be representative for all children within that country. This is particularly true for countries with a high percentage of elite and private schools participating in #DQEveryChild. It should also be noted that the results are combined from 2017 to 2019 as we did not find significant changes over time. Although not strictly a limitation, readers should also be reminded that as with the inaugural COSI, the scores are standardized and relative across the thirty countries to ensure equal weighting among the measures.

# **REFERENCES**

Anders, D. (2019). Internet Speed Classifications | What is a Good Internet Speed?. Retrieved from <a href="https://www.allconnect.com/blog/internet-speed-classifications-what-is-fast-internet">https://www.allconnect.com/blog/internet-speed-classifications-what-is-fast-internet</a>

Anderson, C. A., Berkowitz, L., Donnerstein, E., Huesmann, L. R., Johnson, J. D., Linz, D., Malamuth, N. M., & Wartella, E. (2003). The influence of media violence on youth. Psychological Science in the Public Interest, 4(3), 81–110. https://doi.org/10.1111/j.1529-1006.2003.pspi\_1433.x

Anderson, C., Gentile, D., & Buckley, K. (2007). Violent video game effects on children and adolescents: Theory, research, and public policy. Oxford University Press.

Anderson, C. A., Shibuya, A., Ihori, N., Swing, E. L., Bushman, B. J., Sakamoto, A., Rothstein, H. R., & Saleem, M. (2010). Violent video game effects on aggression, empathy, and prosocial behavior in Eastern and Western countries: A meta-analytic review. Psychological Bulletin, 136(2), 151–173. https://doi.org/10.1037/a0018251

Ang, R., & Goh, D. (2010). Cyberbullying among adolescents: The role of affective and cognitive empathy, and gender. Child Psychiatry & Human Development, 387-397.

Broadband Commission for Sustainable Development. (2019). Child online safety: Minimizing the risk of violence, abuse and exploitation online. Retrieved from: <a href="https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety\_report.pdf">https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety\_report.pdf</a>

Busching, R., Gentile, D. A., Krahé, B., Möller, I., Khoo, A., Walsh, D. A., & Anderson, C. A. (2015). Testing the reliability and validity of different measures of violent video game use in the USA, Singapore, and Germany. *Psychology of Popular Media Culture, 4*, 97-111

DQ Institute. (2019). DQ Impact Report.

Economist Intelligence Unit. (2019). Retrieved from Out of the shadows: Shining light on the response to child sexual abuse exploitation: https://outoftheshadows.eiu.com/

Gentile, D. A., Bailey, K., Bavelier, D., Funk, J. B., Cash, H., Doan, A., Grant, D. S., Green, C. S., Griffiths, M. D., Markle, T., Petry, N. M., Prot, S., Rae, C. D., Rehbein, F., Rich, M., Sullivan, D., Woolley, E., & Young, K. (2017). Internet Gaming Disorder in children and adolescents. Pediatrics, 140, S81–S85.

Gentile, D. A., Lynch, P. J., Linder, J. R., & Walsh, D. A. (2004). The effects of violent video game habits on adolescent hostility, aggressive behaviors, and school performance. Journal of Adolescence, 27(1), 5-22.

Global System for Mobile Communications. (2019, December). GSMA Mobile Connectivity Index. Retrieved from

http://www.mobileconnectivityindex.com/#year=2018&secondaryMenu=about-the-index

ICMEC. (2018). Retrieved from Child Sexual Abuse Material: Model Legislation & Global Review: https://www.icmec.org/child-pornography-model-legislation-report/

International Telecommunication Union. (2018). Retrieved from Global Cybersecurity Index: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

International Telecommunication Union. (2019, December). ITU Committed to connecting the world. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Lemmens, J., Valkenberg, P., & Gentile, D. (2015). The Internet Gaming Disorder Scale. Psychological Assessment, 27(2), 567.

Livingstone, S., & Bober, M. (2004). Taking up online opportunities? Children's uses of the Internet for education, communication and participation. E-Learning and Digital Media, 1(3), 395-419.

Livingstone, S., & Haddon, L. (2009). EU Kids Online. Zeitschrift Für Psychologie/Journal of Psychology, 217(4), 236.

Ookla. (2019, December). Speedtest. Retrieved from Internet speed glossary: https://www.speedtest.net/about/knowledge/glossary

Ookla. (2019, December). Retrieved from Speedtest Global Index: https://www.speedtest.net/global-index

Patchin, J. (2019, July 10). Cyberbullying Research Center. Retrieved from Summary of Our Cyberbullying Research (2007-2019): https://cyberbullying.org/summary-of-our-cyberbullying-research

van den Eijnden, R. J. J. M., Lemmens, J. S., & Valkenburg, P. M. (2016). The Social Media Disorder Scale. Computers in Human Behavior, 61, 478–487. https://doi.org/10.1016/j.chb.2016.03.038