

*Think*Young
What millennials think

DIGITAL RESILIENCE

EMPOWERING YOUTH ONLINE

Practices for a safer internet use.
A major survey targeting Australia, Indonesia, Japan, Korea and Taiwan

Phase I: Asia Pacific (APAC)



*Think*Young
What millennials think

Contents

Executive Summary	4
Part I. Introduction	6
Rationale	6
Research Objectives	7
Report Structure	7
Defining Digital Resilience	7
Survey Methodology	9
Part II. Profiling the Ideal Digitally Resilient Young Person	10
Setting the Scene	10
Definitions	11
Reducing Complexity through Resilience Scores	11
Preventive Resilience Scores	11
Reactive Resilience Scores	11
Emotional Response to Risk: Time Resilience	12
The Online Resilient Young Person – a Graphical Representation	12
Other Country Trends and Rankings	15
Part III. Measuring Digital Resilience	17
Setting the Scene	17
Preventing Risk	17
Instrumental Strategies	17
Behavioural Strategies	17
Responding to Risk	18
Unwanted Disturbing Content	18
Disturbing Messages	18
Misuse of Personal Information	19
Online Approaches and Meeting Requests	19
Cyber-Bullying	21
Comparisons with Previous Findings	21
Part IV. The Policy Challenge	22
Setting the Scene	22
Fostering Digital Resilience: The Role of Media Skills and Digital Literacies	22
Barriers to Resilience	23
Defining Risk, Harm and Vulnerability	24

Empowerment: Balancing Opportunities and Risks	24
Challenges for Internet Governance	24
Regional Frameworks	25
National Level	25
Risk vs. Opportunity: Instruments to Strike the Right Balance	26
Content Blocking Filters	27
School and Education	27
Hotlines and Reporting Mechanisms	27
Extra-Curricular Learning	27
Policy Recommendations	27
Conclusion	28
References	29
APPENDIX A: Resilience Scores	31
APPENDIX B: Determinants of Resilience - Descriptive Analysis	32
APPENDIX C: Tables in the Report	40
APPENDIX D: Age Group Variations in the Adoption of Resilience Strategies	48

Acknowledgements

March 2016

Authors: Michele Rimini, Charles Howard, Alexis Ghersengorin

The following project and its outputs were discussed with ThinkYoung colleagues and benefitted substantially from the help and strategic guidance of Alberto Gerosa. Manon Dené provided invaluable research assistance while Tiffany Palmer and Phyllis Yeung were in charge of the report's layout and design.

Executive Summary

The following multinational research explores the role of digital resilience (the ability to prevent and respond to online risk¹) in providing children with the skills and characteristics needed to navigate the internet safely. Analysing the findings from children aged 9-18 in Australia, Japan, Indonesia, Korea and Taiwan; it investigates the ways in which young people can be encouraged to be resilient users.

In this context, resilience encompasses a set of skills and attitudes allowing a young person to avoid and adapt to risky situations faced online. These range from being able to avoid risk through online awareness and prevention, the ability to be unfazed by risk, and the competence in using strategies to respond to risk. These strategies include ignoring the risk, communicating the risk or using proactive digital skills to resolve the risk (deleting, blocking or reporting the person/problem).

The main findings highlight the following:

Overall Findings

Children use a variety of digital skills to prevent and respond to online risk including: using child friendly search engines, having filters and software that protects from unwanted content or contacts, managing their profile settings, cautiously managing their online contacts and carefully using their passwords. In particular the findings of this report suggest that:

- 85% of children are likely to keep their password completely secret and 70% are likely to modify privacy settings to avoid unwanted content.
- When responding to risk young people are confident using digital skills, with 66% changing their password when personal information is misused.
- Young people show a critical awareness in their use of the internet, with 52% careful about what they say or post online, and 55% avoiding suspicious material.

- Young people above 16 years old are more likely to use technical/digital skills to respond to risk than their younger fellows.
- Frequent use of the internet (time and range of uses) increases risk exposure yet builds resilience - as greater internet use fosters improved navigational skills and online awareness.

National Findings

- Young people in Australia score the highest for instrumental strategies and rank also second for disengaging with risk, avoiding risk through an awareness of online content and in seeking advice for communicating a problem.
- On the whole, Indonesian children rank above average for all aspects of digital resilience. They rank second for using digital skills to respond to risk and rank first for communicating risk and seeking help from a friend or guardian
- Japanese children score below average for disengaging with risk, and more generally they score low across the board, ranking last for communicating a problem, for engaging critically with risky content and contacts online, and last for using digital skills to respond to risk.
- In general, as for Japanese children, Korean children score low across the board. They display lower than average levels of cognitive resilience by ranking 4th in this respect. They also score very low for seeking advice from parents, guardians or friends. They however score above average for adopting confrontational strategies.

¹The term risk refers to all situations in which children can be affected by negative behaviours including: exposure to pornographic content, being bullied, harassed or stalked, receiving unwanted sexual comments and meeting an online contact offline.

- Taiwanese children score the highest regarding disengagement strategies. Moreover, although they rank third, they fare about average in adopting behavioural preventive strategies. They are also more likely than the average to adopt communicational skills, and more precisely their score in reaching out to parents, siblings or peers is relatively high.

- In all countries, frequency of internet usage is associated with higher levels of risk avoidance through awareness, digital skills and likelihood to communicate and seek help from others while facing risk.

Policy Recommendations

Based on the research also showing children self-regulating their internet usage, and formal and informal education being the best means for learning online skills, this study recommends to:

- Promote the inclusion of digital literacy and internet safety education into school curricula from early childhood education, and to ensure the provision of ICT training for teachers and educators.

- Foster extra-curricular activities aimed at promoting responsible and mutually respectful internet use.

- Improve and promote the existing hotline support services as a more reliable means to convey child concerns, and to report problems

- Secure a free and open internet for children that allows them explore and make the most of its opportunities, while educating them and building resilience in them to the risks online.

Part I. Introduction

Young people are living in an age of unprecedented developments in information and communication technology (ICT), with more and more children actively using the internet as means for both educational and social participation. As such, the use of technologies has quickly become a deep-rooted infrastructure of everyday life, whether through direct engagement with ICT or through the institutional management of contents and services affecting the conditions of children's lives (Livingstone, 2014a). New technologies coupled with increasing levels of interconnectivity inevitably have a wide range of benefits for young people, ranging from education and learning to civic participation and self-expression.

However, the characteristics making the internet a tool for creativity, learning and exploration, also come with certain levels of risk for the user. As a result, questions of how best to keep children safe when online but also free to access and use the internet in a way for both individual empowerment, and for actively seeking and benefiting from the opportunities available, are becoming increasingly important on a global policy and regulatory scale.

Despite the widespread acceptance that risks and opportunities when online are often interrelated, the debate has largely been overshadowed with maintaining security and preventing risk for young people. Equally prevalent is the fact that on the whole, parents, teachers and policy makers are often ill informed about the associated risks and opportunities the internet provides. Whilst a significant amount of attention has been placed on promoting safety online, it has been noted that these safety initiatives to reduce risk often negatively impact the opportunities present, including socialising, and learning and self-expression, through measures that overly restrict access.

As a consequence, it has become increasingly apparent that alternative strategies are needed in order to move beyond the prevalent viewpoint that risks and opportunities online are in opposition. According to Davies (2011 p.1) with reference to the online lives of young people, 'safety must sit alongside, and be integrated with, a broader range of considerations, including promoting positive uptake of online opportunities'. A key element of this is in the promotion of competencies relevant to the digital economy.

Rationale of this Study

While advocates of online child protection and freedom of expression share a concern for the protection of rights online, they often find themselves in perceived (and real) opposition in the actual practice of law, policy and regulation (Hills et al., 2010). Moving beyond this fragmented outlook has resulted in an understanding that fostering greater levels of individual resilience to the material to which they may be exposed can create the confidence and skills required to navigate new media waters more safely (Byron, 2008).

With this in mind, the following multinational report will seek to define and investigate the role of digital resilience in positively impacting children's online engagement. Moreover it will shed light on how a digitally resilient young person responds to risky online content, and how this can be further developed on an international scale through the promotion of enhanced online skills.

Lastly, in light of the complex nature of child safety online and based on the large gaps present in global research, there is a need for 'more country-wide as well as region-wide research targeting early childhood and school-aged population' (UNESCO 2014, p. 14). This report aims to add to this international evidence base through the investigation of children's digital resilience (9-18 years of age) through the analysis of empirical data from Australia, Japan, South Korea, Taiwan, and Indonesia.

Research Objectives

With reference to the key debates on child internet safety and in line with the theoretical framework of digital resilience outlined by previous scientific literature, this research aims to empirically grasp which characteristics are most fundamental within the ideal digitally resilient young person and to establish a novel approach for measuring digital resilience.

Based on the survey administered, with a focus on how young people respond to risk, the types of risk encountered, their computer literacy and digital skills, and their preferred methods of ICT education, this research has further sought to understand:

- The impact of awareness and self-regulation in understanding the potential for risk when online, and in critically engaging with online content in a resilient way.
- In responding to risk, how children and young people can enhance their levels of resilience through communication and the seeking of advice.
- How media skills and digital literacies improve levels of resilience, and which types of response to risk are employed by technologically advanced young people.

Report Structure

The first stage of this analysis (Part I) will begin with an overview of digital resilience and its key debates, presenting the characteristics of a digitally resilient young person. In light of the theoretical approach and of the results of the ThinkYoung survey, Part II will illustrate the profile of an ideally resilient young person by presenting national resilience scores and comparing how each country fares in comparison with the model digitally resilient young person.

Part III will describe in more detail this novel approach for measuring digital resilience by illustrating the varying resilience strategies employed by young people in response to the risks faced online. Part IV will explore the key debates on child online safety to illustrate how it can be addressed by policy makers. This will introduce the international, regional, and national policy context with policy recommendations presented in light of the results of this project.

Defining Digital Resilience

The role of digital resilience as a means for children and young people to safely navigate the internet, self-regulate content, and respond to the potential risks and harm when online is becoming increasingly prevalent. According to the Byron Review (2008)² building resilience is a key objective promoting children's ability to manage risk.

Preventing risk is a key aspect of resilience, whereby an understanding and awareness of the potential for harm when online and being able to effectively self-regulate media usage positively affects resilience levels. Moreover, young people with "autonomous self-regulation" (the ability to manage short and long-term desires according to individual values) (Donoso et al., 2013) are empowered to use the internet to acquire knowledge and to take advantage of digital technologies (Linington and Mishkin 2014).

While employing preventive measures (awareness and self-regulation) are integral to avoiding risk and in being resilient, the ability to respond to, and cope with risk is equally important. According to Bartley (2006): 'The notion of resilience refers to the process of withstanding the negative effects of risk exposure, demonstrating positive adjustment in the face of adversity or trauma, and beating the odds associated with risks' (p. 4).

²The Byron Review was an independent report commissioned by the Prime Minister of the United Kingdom in 2007 reviewing the risks children faced from both the internet and video games. The recommendations of the review were accepted by the British government, which led to the establishment of the United Kingdom Council for Child Internet Safety (UKCCIS).

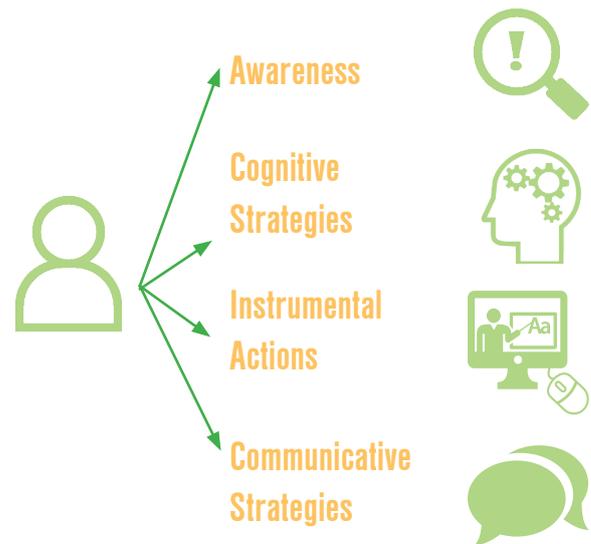
As a result, young people who are labelled as digitally resilient are also able to deal with negative experiences online, tackle adverse situations and experiences in a problem-focused manner, and turn negative emotions into positive (or neutral) feelings (Donoso et al., 2013). This is fundamental for young people, particularly in an 'always on' digital world where children must be empowered with the capacity to judge and respond to risk independently (Linnington and Mishkin 2014).

The concept of digital resilience thus encompasses both a preventive and reactive phase, where at first young people are able to self-regulate and avoid online risk and, when faced with risk, are able to employ coping mechanisms in order to respond to the risk or harmful situation in a problem focused manner.

As conveyed in Fig.1, a digitally resilient young person harbours the following set of skills and characteristics fundamental in navigating the internet in an empowered manner and in responding to online risk:

- An **Awareness** and understanding of the risks present.
- The use of **Cognitive Strategies** and development in order to critically engage with online content, and to foster problem solving and decision-making.
- The ability to employ **Instrumental Actions** to cope and respond to risk through the use of digital skills and media literacies.
- The willingness to **Communicate** with people when faced with a risky, upsetting or potentially dangerous situation online.

Figure 1. The Digitally Resilient Young Person



This set of skills and attributes allows a young person to critically engage with online content in a safe and self-regulated way. This is further translated into the young person's ability to both self-monitor their activities, recognise where potential danger may be, and refrain from taking part in risky online practices.

Moreover, in responding to actual risk, these skills and strategies equip young people with the necessary tools to address the risk and prevent harm from taking place. As Donoso, d'Haenens and Vandoninck (2013) note, these coping strategies can range from passive reactions to risk (ignoring the problem), to communicative measures (talking to someone) and proactive measures (fixing, deleting or blocking the problem/person).

Survey Methodology

The data collection exercise was performed between May and June 2015 through an online survey administered amongst children and young people aged 9-18. The survey reached a targeted audience of 500 respondents for each country involved in the study (Indonesia, Japan, Korea, Australia, Taiwan) for a total of 2600 respondents. In order to guarantee the sample's representativeness mild population adjustments were performed using tables from UNDESA World Population Prospects: The 2012 Revision (Medium variant).

The questionnaire was prepared in two versions: the first was directly administered to children aged above 16 and the second was administered to parents who allowed their children to partake (9-16).

In gaining parental permission for the 9-16 year olds, a very clear statement of intent was given to parents/guardians in advance, outlining the exact purpose of the study, sharing the exact questions and giving assurances that the data would be treated anonymously.

The wording of the questionnaire was refined on the basis of cognitive testing with children and on a consultation with a team of secondary school teachers in order to avoid adult terminology and to ensure children's comprehension. Moreover, particularly sensitive terms such as "naked", "bully" or "sex" were avoided. The survey went to a field trial process before going live to ensure respondents' uptake.

The questions were framed in mutually exclusive and mutually non-exclusive terms. When appropriate a Likert scale was adopted.

The statistical analysis was performed using SPSS, Gretl and STATA. Standard statistics for normality and correlation were employed. Correlation and significance were tested using T-test, Analysis of Variance (ANOVA) and F-test as well as Chi square test.

Part II Profiling the Ideal Digitally Resilient Young Person

Key Messages

The following section presents an analysis of the survey's results from each country in the format of an overall national score of resilience, based on a predefined set of resilience strategies (preventive and reactive). This score also takes into account the time it takes for children to get over/recover from a negative online experience. According to the results:

- Children in Australia score the highest for instrumental strategies and rank also second for disengaging with risk, avoiding risk through an awareness of online content and in seeking advice for communicating a problem.
- Children in Indonesia rank second for using digital skills to respond to risk and rank first for communicating risk and seeking help from a friend or guardian.
- Japanese children score below average for disengaging with risk, and more generally they score low across the board, ranking last for communicating a problem, for engaging critically with risky content and contacts online, and last for using digital skills to respond to risk.
- In general, as for Japanese children, Korean children score low across the board. They display lower than average levels of cognitive resilience by ranking 4th in this respect. They also score very low for seeking advice from parents, guardians or friends. They however score above average for adopting confrontational strategies.
- Taiwanese children score the highest regarding disengagement strategies. Moreover, although they rank third, they fare about average in adopting behavioural preventive strategies. They are also more likely than the average to adopt communicational skills, and more precisely their score in reaching out to parents, siblings or peers is relatively high.

Setting the Scene

This chapter aims to provide an overview of the key findings with reference to youth attitudes towards preventing and responding to online risk. It adopts a country level approach where the different responses to the survey are clustered into resilience scores. Resilience scores help in identifying the profile of the ideal digitally resilient young person, defined as the person who adopts the widest amount of strategies to safely use the internet without giving away his or her personal freedom.

The definition of resilience scores is instrumental in unveiling international key trends. It also enables cross country comparisons to be made whereby each country can compare the performance of its children to that of other countries - thus assessing its relative strengths and weaknesses.

Definitions

In order to safely navigate the web and take advantage of the wealth of information and opportunities available, children can put in place strategies to minimise their exposure to online risk. The literature defines those strategies as preventive insofar as they don't result as a response to harmful situations.

For the purpose of this study and, in accordance with the existing literature, a list of preventive strategies for digital resilience has been identified along the macro categories of instrumental (using specific technical instruments to avoid risks) and behavioural (avoiding risks through specific safety behaviours).

In a similar fashion, another strand of literature (Luthar, Cicchetti and Becker, 2014) also defines resilience as the ability to deal with negative experiences online or offline. According to this perspective resilient children are able to tackle adverse situations in a problem-focused way, and to transfer negative emotions into positive (or neutral) feelings.

This study identifies this approach as reactive as opposed to preventive with the goal of measuring how children react to specific online risky situations such as exposure to sexual content, cyber-bullying and security frauds, among others.

The ensuing definition of reactive resilience is further separated into 4 types of attitudes that children may adopt: instrumental measures, confrontational measures, other-reliant communicative strategies or disengagement strategies.

With instrumental measures children master the tools that help them navigate safely in response to a certain risky situation. As an example, they may block a contact who teases them. Confrontational measures are strategies where the child engages in personal confrontations with the stressor or aggressor by asking him or her to stop. Other-reliant/communicative strategies are those situations where the child asks for help from family, friends or institutions to deal with risk and harm. Lastly, disengagement strategies reflect an approach that tends to minimise the importance of risk and harm by mainly ignoring the harmful content or contact and thus avoid any risky interaction.

Lastly and in line with a more traditional and overarching definition, resilience is also measured as the ability to quickly reabsorb from the shock of a negative online experience.

A detailed description of the most prevalent preventive and reactive strategies at international and national level with reference to online risk will be provided in Part III of this report.

Reducing Complexity through Resilience Scores

With the aim of reducing complexity and to extrapolate a meaningful correlation analysis, the three types of resilience previously outlined have been translated into corresponding scores. The next section briefly illustrates how this has been achieved.

Preventive Resilience Scores

The notion of preventive resilience has been reduced to a double score capturing the dimension of both technical and behavioural preventive strategies. Each child obtains a score from 0 to 3 depending on how many technical and behavioural strategies he or she is likely to adopt.

Reactive Resilience Scores

Reactive resilience has also been reduced to four scores that reflect the distinctions highlighted by previous research on which the survey has extensively drawn from. As a result the following scores ranging from 0 to 3 have been created:

- Instrumental coping resilience score
- Confrontational resilience score
- Communicative resilience score
- Disengagement resilience score

Emotional Response to Risk: Time Resilience

The time resilience score corresponds to the answer to the question: If you are ever upset by things that happen on the internet, how long does it tend to upset you for? It ranges from 0 to 3 where 3 corresponds to being upset for hardly any time by things happening on the internet.

For the sake of having a reduced number of metrics to compare countries' resilience levels, preventive and reactive resilience scores have been combined to give better insights to policy makers as to what levers should be used to foster digital resilience. As a result the analysis unfolds according to the following scores:

1. Cognitive score
2. Instrumental score
3. Communicative score

The cognitive score summarise the likelihood of adopting behavioural preventive strategies such as being careful about what one posts about him or herself as well as the likelihood to adopt disengagement strategies when facing risk (e.g. ignore a bully).The cognitive score captures the extent to which young people are both aware and can critically reflect about online risk.

The instrumental score comprises all the instances in which the child uses his or her digital skills to prevent or get rid of the incoming risk or threat.

The communicative score represents the likelihood of a young person to reach out to others (parents, siblings, teachers or institutions) when facing online risk and to confront aggressors and stressors (e.g. bully).

The Online Resilient Young Person – a Graphical Representation

The graphical representations below illustrate how well children in each country fare in comparison with an ideal digitally resilient young person, who would score 3 points in each dimension.

Figure 2. The Resilient Young Person in Australia



In comparison with the other surveyed countries Australian children obtain top scores in terms of cognitive resilience (2.16) far above the average of 1.98. On the assumption that an ideally resilient young person would adopt all preventive behavioural strategies and will disengage with risk and confrontations (unless they are causing actual harm), the average young Australian ranks at 72% compared to the ideal digital citizen in terms of cognitive resilience, compared to an overall average of 66%.

This score is further illustrated by the top performance of Australian children as to the adoption of disengagement (1.65) and behavioural preventive strategies (2.66) where they both rank second.

Similarly, Australian children (1.82) score above average (1.61) with regard to instrumental resilience, meaning that they tend to use most of the available technical instruments to prevent and cope with online risk. Thus the Australian child receives a 62% score in reaching the ideally resilient young person in terms of instrumental resilience.

Lastly, Australian children (0.98) rank second in terms of communicative resilience far above the average score (0.82). This result is explained by a score in the adoption of communicative strategies of 1.05 and 0.91 with regard to the adoption of confrontational strategies.

Figure 3. The Resilient Young Person in Indonesia



Indonesian children (1.97) fare about the average (1.98) in terms of cognitive resilience. This result places them at 66% or 34% distant from the ideally resilient young person according to this parameter. The score however results from a relatively strong performance in the adoption of preventive behavioural strategies (2.62) and a relatively poor performance with regard to disengagement strategies (1.32) where Indonesian children rank last.

Children in Indonesia do however score high (1.82) in terms of instrumental resilience, ranking 2nd among the surveyed countries and placing themselves 39% away from the ideally resilient young person.

Indonesia ranks first when it comes to communicative resilience (1.06). This result is mostly explained by the high levels registered with regard to the uptake of confrontational strategies (1.29), well above the average level across APAC countries (0.87).

Figure 4. The Resilient Young Person in Japan



Compared with other countries, children in Japan demonstrate lower levels of cognitive resilience (1.77) ranking last among the other surveyed countries, far below the country average (1.98). This level indicates that Japanese young people are 41% away from the ideal digitally resilient young person with respect to this parameter. The cognitive resilience score reflects a low score regarding the adoption of behavioural preventive strategies (2.16) and a below average score in disengagement strategies (1.38).

Japan also ranks last in reference to instrumental resilience with 1.21 points. This is quite far from the profile of the ideally resilient young person and well below the average for APAC countries (1.61).

Similarly, Japan ranks last also with respect to communicative resilience with 0.44 points, indicating that Japanese children are little inclined to confront the perpetrator, or to communicate with parents, siblings and peers when they encounter online risks.

Figure 5. The Resilient Young Person in in Korea



Korean children display lower than average levels of cognitive resilience (1.80 vs. 1.98) by ranking 4th out of the 5 countries in this respect. However, in terms of distance from the ideally resilient young person this result is somewhat encouraging as it reflects a 60% level of completion on this specific factor.

Korean children rank below average also in terms of instrumental resilience (1.46 vs. 1.61), situating themselves approximately half way on the path towards the ideally resilient young person in this respect.

In terms of communicative resilience Korea ranks below average (0.71 vs. 0.82). This ranking illustrates two different tendencies where Korean children are more likely than the country average to confront their stressors or aggressors (0.83), yet are less likely to reach out to parents, siblings or peers (0.47)

Figure 6. The Resilient Young Person in Taiwan



Taiwanese children obtain top scores along the dimension of cognitive resilience (2.21) situating themselves at 74% on the path towards the ideally resilient young person. The score reveals two tendencies where young Taiwanese people are more likely to adopt disengagement strategies (1.82) than the rest of the sample but only fare about average in adopting behavioural preventive strategies (2.59).

Taiwanese children (1.74) obtain slightly above average scores (1.61) in terms of instrumental resilience displaying a good score (58%) when compared to the ideally resilient young person.

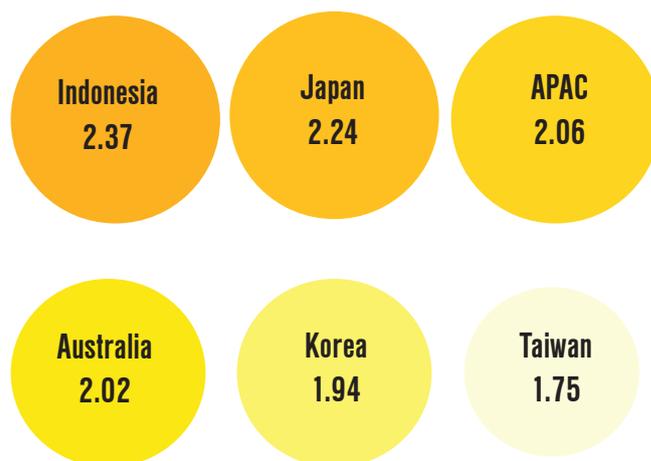
Children in Taiwan display higher than average scores with regard to communicative resilience (0.89). Their score in reaching out to parents, siblings or peers is relatively high (0.87 vs 0.76) compared to the average among APAC countries as it is the score (0.91 vs 0.87) relative to the extent to which Taiwanese children confront their stressors or aggressors.

Other Country Trends and Rankings

The section above illustrated how resilience can be measured and ranked according to different criteria. Overall country trends suggest that children in some countries are more resilient than others. This is the case of Australian children who rank significantly above the average of those from other countries in all measures of preventive and reactive resilience (the complete rankings are displayed in appendix C). On the contrary, children in Japan consistently rank at the bottom of all indicators of preventive and reactive resilience with the exception of those related to disengagement strategies. Indonesian children obtain top scores with regard to instrumental and communicative resilience.

Lastly, and in light of previous research carried by Donoso et al. (2013), it is worth analysing how countries fare with regard to time resilience, defined as the extent to which children are affected by disturbing experiences over the internet as illustrated in Table A. Indonesian young people are those who are affected the least from bad things happening on the internet as 53% of them report to be affected for hardly any time by these experiences. On the contrary, Taiwanese children tend to be affected to a larger extent when facing situations of online risk as only 23% report being unfazed by online risk/harm. The emotional dimension of resilience is therefore better mastered in countries such as Japan and Indonesia compared to Korea and Taiwan. Interestingly and somewhat intuitively this ranking mirrors what is found for disengagement resilience with Taiwan at the top and Indonesia at the bottom.

Table A: Time Resilience across Countries



Part III Measuring Digital Resilience

Key Messages

Child online resilience (the ability to avoid and overcome risky and harmful situations when online) can take many forms. At the preventive stage children use a broad spectrum of technical instruments and behavioural strategies.

Children display relatively high levels of instrumental action take up with 52% of them very likely to keep their password completely secret from anyone; only 33% however are very likely to modify privacy settings to be kept away from unwanted content.

At the same time, for the most part children are acquainted with the “think before you post” principle and avoid certain risky practices. 52% of children report to be careful about what they say and post about themselves, while 55% avoid clicking on things that look strange or suspicious.

With reference to all but online approaches and meeting requests, children mostly use instrumental techniques such as closing the page containing unwanted content (59%), deleting or blocking the contact who cyber-bullies them (43% and 45% respectively) and changing the password when personal information is stolen or misused (49%).

The majority of children adopt disengagement strategies when they are approached online by strangers, with 51% ignoring the contact. Children also mostly refuse to meet (54%) an online contact who wants to meet them in person/in an offline context.

Communicative strategies are widely used in instances of exposure to disturbing content, cyber-bullying as well as online approaches and meeting requests. The relative preponderance of communicative strategies holds in instances where children are actually exposed to personal information misuse and to online approaches and meeting requests.

Setting the Scene

This chapter aims at further illustrating the varying resilience strategies employed by young people when confronting online risks. The survey respondents were asked to detail their likelihood of adopting strategies to prevent online risk and to describe what strategies they would be likely to employ when facing online risk (reactive strategies). The chapter thus provides the reader with a comprehensive overview of the most frequent attitudes of young people in Australia, Indonesia, Japan, Korea and Taiwan in dealing with online risk.

Preventing Risk Instrumental Strategies

International Analysis

The responses to the ThinkYoung survey highlighted a relatively high uptake of instrumental actions across countries from the group Asia and Pacific where, as an example, 33% of children said to be very likely to modify privacy settings to be kept away from unwanted content (37% are fairly likely), as well as being very likely to use complicated and safe passwords (34%). Similar levels of agreement are found with behaviours such as turning off programmes considered risky (39%) and keeping passwords secret from anyone (52%).

The practices of using child friendly search engines (52% likely vs. 39% unlikely) and of using a secondary account for spam and other emails (53% likely vs. 36% unlikely) are less widespread among children aged 9-18. Full results are displayed in table 1 in appendix C.

Country Level Analysis

The analysis conducted at country level does not show substantial differences when considering the overall likelihood of undertaking specific instrumental actions. Child attitudes towards making a profile unavailable, and privacy and password settings are very much similar across countries. Different attitudes among countries are, however, displayed with regard to the usage of child friendly search engines. As an example children in Japan (32% likely vs. 47% unlikely) South Korea (42% likely vs. 40% unlikely) and Australia (43% likely vs. 50% unlikely) are less inclined to adopt this practice than their peers in Indonesia and Taiwan, as illustrated in table 2 in appendix C.

Similarly, children in Japan (47% likely vs. 29% unlikely) and South Korea (48% likely vs. 33% unlikely) are less inclined than their peers in the other surveyed countries to use filters and software that protects them from unwanted content (on average 63% likely vs. 26% unlikely).

Frequency of Internet Usage

Intuitively, frequency of internet usage is associated with higher levels of familiarity with the tools enabling a safer navigation. As we can see in table 3, this result holds for the ThinkYoung sample where a higher level of internet usage is significantly positively correlated³ with: a) activating filters protecting from unwanted content, b) turning off programmes considered risky, c) using a secondary email account, d) using complicated passwords.

Socioeconomic Status

Socioeconomic status is positively correlated with the adoption of technical preventive strategies. The correlation is significant for each of the considered actions, with the exception of turning off programmes that are considered risky.

Behavioural Strategies

International Sample

The adoption of behavioural strategies to prevent online risks has been analysed in the survey through the perspective of self-monitoring activities reflecting the “think before you post” principle and behavioural avoidance - staying away from certain risky practices.

The international sample illustrates widespread adoption of behavioural preventive strategies where the most common practices across children are: a) to avoid clicking on things that look weird or suspicious (55% of children who agree with the statement), b) to be careful about what they say and post about themselves (52%) and c) to only share things with close friends (51%).

Country Level Analysis

On a country level, no significant differences are observed with regard to specific behavioural strategies. It is however the case that children in Japan and Korea display a lower disposition to adopt preventive behavioural strategies than their fellows in Australia and Indonesia. This is well illustrated in the example below where Korean (31%) and Japanese (42%) children are less inclined than the average for our 5 countries (52%) to be careful when talking and posting about themselves, as we can see table 5 of the appendix C.

Gender Differences

The gender differences analysis on behavioural preventive strategies demonstrates that girls are more inclined to adopt these strategies than boys. This result holds for all behavioural strategies but the carefulness in accepting friendship requests where no significant differences are registered. The largest difference (12%) between girls and boys is found with regard to not taking provocative pictures or undress in front of the webcam, where girls recognise the statement to be very true in 88% of the cases when compared to 76% registered by boys.

³A one way Anova test has been conducted to detect significant associations

Frequency of Internet Usage

In line with the results on technical preventive strategies, the analysis of behavioural preventive strategies shows significant and positive correlation between these and the frequency of internet use. This result holds for all the surveyed strategies except from avoiding clicking on pop-ups or websites that look strange or suspicious.

Socioeconomic Status

The adoption of the previously discussed behavioural preventive strategies is also positively correlated with a child's socioeconomic status across countries and age groups. The strength of this correlation is remarkable when the practice of covering the webcam is taken into consideration.

Responding to Risk

The analysis of reactive resilience will be therefore conducted following the risk/reactive strategies matrix (fig. 2)

With the aim of collecting the largest amount of responses, the questions were asked in an hypothetical way so that children who had not experienced certain risky or harmful situations were also able to express their opinions on the strategies they would be more likely to adopt.

Figure.2. Reactive Resilience Matrix

	Unwanted disturbing content	Disturbing messages	Misuse of personal information/ pictures	Online approaches and meeting requests	Cyber-Bullying
Instrumental					
Confrontational					
Communicative					
Disengagement					

Unwanted Disturbing Content

Surfing the web constitutes a great opportunity for children to learn and explore an unprecedented amount of information, images and multimedia content. However, as previously mentioned in this report, this freedom entails the possibility of incurring disturbing content of a sexual/ violent or inappropriate nature. When this happens children can adopt a handful of strategies to cope with these specific risks, along the macro-categories identified above.

International Sample

The first level of analysis is conducted on the international sample including all age groups. The results highlight that the most widespread strategy when incurring in unwanted content is to immediately get rid of it (59%) followed by the more technically sophisticated measure of blocking the perilous website (29%) and by asking parental advice (26%). Thus instrumental and communicative strategies are predominant in this case.

International Sample – Children Exposed to Unwanted Disturbing Messages

The consistency of responses was tested by restricting the analysis to the sample of those children who reported to have incurred in unwanted sexual or violent content. Results in table 7 in appendix C illustrate that the theoretical approach of what the children would do is reflected in the actual behaviour of children who have experienced that situation. The only exception relates to communicative coping strategies where only 18% of children ask for parental advice. 23% however talk about it with a friend.

Country Level Analysis

The country level analysis demonstrates the existence of significant country differences with regard to the extent to which children would reach out to their parents when seeing disturbing content online. This difference is particularly remarkable when data from Australia (45%) and Japan (16%) are compared. Children in Indonesia (21%) tend to be more indifferent to this risk as they keep watching the unwanted content.

Disturbing Messages

International Sample

While the opportunities the internet provides are widespread, with socialising and communicating being two of the most commonplace activities undertaken by children and young people, certain risks are exacerbated. Amongst the potential risks faced for young people online, receiving unwanted or disturbing messages is one of the most prevalent encountered in our sample (38%).

Taking into account the responses from the entire sample internationally, and using the macro category of coping strategies detailed previously, the most common response to disturbing messages for children and young people is to ignore the message and/or person (47%), closely followed by deleting the contact in question (40%), and blocking or reporting the person (37%). As a result, instrumental and disengagement strategies are the preferred tactic for responding to this risk.

International Sample –Children Exposed to Unwanted Disturbing Messages

When the theoretically preferred strategies responding to disturbing messages are compared to the actual results from the respondents who had experienced this risk, the same strategies are adopted. However, the percentage of respondents adopting instrumental and disengagement strategies is slightly higher, with 60%, 52% and 52% respectively. We can also note that children who actually received disturbing messages talk less about it to their parents (20%) than they would theoretically do (34%), and ask more frequently the person to stop sending annoying messages or to delete an embarrassing picture (33% vs. 21%).

Country Level Analysis

Taking into account country variations it is interesting to note that children in Japan (22%) and South Korea (35%) are less likely to adopt instrumental coping strategies when compared to their Australian counterparts (52%). Moreover, children in Indonesia are more than 6 times as likely to ask the person to stop messaging them (confrontational strategy) when compared to children in Japan.

Misuse of Personal Information

Information, privacy and security concerns are a further category of risk faced when online, with the giving out and misuse of personal information a key priority for internet policy stakeholders. As a result, cybercrime and e-security concerns have been prevalent in a number of research initiatives on child online safety. The misuse of personal information, however, is the least encountered risk with only 10% of children and young people having had their password used without their permission and 9% having had someone use their photos.

International Sample

When responses from the entire sample are analysed the most prevalent reactive strategies are instrumental, whereby children and young people are most likely to either change their password (49%) or review their privacy settings (34%). Communicative strategies (28%) are the second most likely cluster of strategies adopted by young people. Confrontational strategies are the least likely to be employed with only 5% of children and young people stating they would politely ask for the account back.

International Sample –Children Exposed to Misused Information

In line with previous trends a higher percentage of respondents who had incurred the misuse of personal information adopted instrumental techniques, with 66% changing their password and 55% reviewing their privacy settings. Interestingly, only 15% of children adopted communicative strategies compared to 28% who stated they would. Confrontational strategies are adopted at 14%, and providing false data is the least common reaction (9%).

Country Level Analysis

Important distinctions are present when the country level responses are compared, with children from Indonesia adopting high levels of instrumental strategies: 60% say they would change their password, and 44% that they would review privacy settings and choose a safer password. Australian children were also the most likely to use communicative strategies with 42% stating they would seek help from a parent or guardian. Japanese children were the least likely to adopt any form of strategy (password change (36%), privacy review (18%), asking to remove the photo or tag (2%) or politely ask for the account back (0%).

Online Approaches and Meeting Requests

Meeting an online contact offline, or receiving messages from an unknown person are both internet risks of particular concern for policy makers, teachers and parents. As a result the following analysis has been split into reactive strategies based on the child or young person receiving messages from an unknown person, and strategies for responding to a request to meet in person or in an offline context.

International Sample

According to the international sample (all age groups) in response to an unknown person engaging in online contact, the most prevalent strategy is to ignore the person (51%), followed by asking parents/guardians if they know the contact (26%) and asking their friends if they know the contact (22%). In response to an invitation to meet an online contact offline, the most widespread strategy is to refuse to meet (54%) followed by seeking advice from parents (31%) and agreeing to meet only if a friend would also go (16%).

International Sample – Children Exposed to Online Approaches and Meeting Requests

The results are somewhat similar amongst the children and young people who had encountered these risks, with 47% ignoring the person and 38% asking their friends if they know the contact. It is interesting to note an important difference: 39% actually replied to the unknown contact (confrontational strategy) but allowing him to see a limited profile (instrumental technique), whereas only 20% stated that they would do so. Another difference can be observed: fewer of the exposed children asked their parents if they knew the person (15% vs. 26%).

Country Level Analysis

In response to unwanted approaches online, the country level analysis again raises important variations between the reactive strategies employed, with Taiwanese children (69%) being nearly twice as likely to use disengagement strategies (ignore the person) when compared to children in Indonesia (35%). Accompanying this, only 5% of children in Japan would ask a friend if they knew the person, compared to 31% in Indonesia, and 22% on average. Crucially, only 6% of children in Australia and Indonesia stated they would reply to the message, compared to 35% in Indonesia. Indonesian children are also the most likely to reply to a message while using instrumental strategies (46% would reply while limiting their online profile).

Country Level Analysis

With reference to responding to requests from a stranger to meet in an offline context the most notable differences exist in the extent to which children and young people would refuse to meet the contact. This is most prevalent when the data from Australia (73%) and Indonesia (33%) is compared. Children in Indonesia (26%) and Taiwan (27%) are also the most inclined to meet a contact as long as a friend is present. 28% of the Indonesian children also accept the contact with a person of a similar age (vs. 4% in Australia).

Cyber-Bullying

A final contact risk present for children and young people when online, as demonstrated in the literature section of this report, is the possibility of being bullied, harassed or stalked.

This risk is particularly felt in the older age group as illustrated by recent statistics coming from the nationwide Australian Covert Bullying Prevalence Survey in 2009 (UNICEF, 2012). As an example, the Australian survey found that rates ranged from 4.9% of students in Year Four (aged 8 to 9) and 7.8% in Year Nine (aged 13 to 14).

International Sample

Using the entire sample surveyed the most commonplace preventative strategies used are to either block and report the person (45%) or delete the contact (43%). As a result, instrumental strategies are the most prevalent when responding to this risk. While communicative strategies are the third most popular method (38% for talking with a parent or guardian), communicating the problem to siblings (13%) and teachers (13%) are viewed much less favourably. Reporting the issue to the police is the least used strategy.

International Sample –Children Exposed to Cyber-Bullying

Testing the consistency of responses by restricting the sample to those who had actually experienced the risk both reinforced the theoretical approach taken and highlighted differences in actual conduct. While the top two strategies of deleting the contact (63%) and blocking the person (54%) are the same (albeit higher), the use of communicative strategies is lower at 22% (talk with parents). Moreover, a higher number of children and young people used confrontational strategies (38%) by asking the person to stop sending messages (compared to 19% in table 22 appendix C). Moreover, the third most popular strategy among the children exposed to cyber-bullying is to show the person they are not bothered by their behaviour (39%).

Country Level Analysis

The country level analysis reiterates the disparity in reactive strategies used by children in Japan and Indonesia, with 56% of children in Indonesia deleting the contact compared to only 26% in Japan. Fewer South Korean children also use instrumental techniques with 37% deleting the contact.

Children in Australia are the most likely to use communicative strategies by talking with parents or guardians (50%) while the Taiwanese children are the most likely to report the problem to the police (14%) and to show the person they are not bothered (38% vs. 22% in Japan).

Comparisons with Previous Findings

In general, a common finding of previous initiatives on child online safety conclude that the risks children are likely to face when online are not significantly different from those faced offline (Hills et al., 2010).

Moreover, it is concluded that the prevalent risks for children and young people are not the same for all children, a finding reiterated in the results of this study.

It is interesting to note that, and in line with the overall findings of the EU Kids Online initiative, the results demonstrate a trend whereby older children are more likely to adopt instrumental or proactive measures in response to risk (deleting or blocking the problem/person). Moreover, female children were more likely to communicate risk when compared to their male counterparts (Haddon and Livingstone et al., 2011). In line with the findings from the SAFT and UKCGO projects conducted in Norway, Ireland and the UK, the results identify older teens as more likely to meet online contacts offline (despite being a low percentage in general). The UKCGO project also concluded that young people who used the internet more (in time spent and range of uses), and those who were more technically skilled, came into contact with more risks.

Interestingly, and as mentioned previously in the analysis section, the results of this project suggest that children who spend more time online are more likely to adopt a variety of coping mechanisms and reactive strategies when faced with risk, and are therefore better able to respond to risk and minimise harm – demonstrating higher levels of digital resilience. This is particularly important as, according to the UKCGO project, young people who use the internet more frequently and who harbour more technical skills, come into contact with risk more often (Livingstone and Staksrud, 2009). This suggests a positive correlation with previous findings whereby children who come across more risk based on increased levels of digital skills and time spent online, are also more resilient.

Part IV

The Policy Challenge

Setting the Scene

This chapter aims to shed light on the existing trade-offs and explore the existing international good practices among policy responses to the challenge of ensuring child safety online. Moreover the ambition of this chapter lies in incorporating the model of a digitally resilient young person in the current policy debate on the instruments for fostering child digital resilience.

Fostering Digital Resilience: The Role of Media Skills and Digital Literacies

As it has been noted, children are able to rely on a number of coping strategies in response to actual and/or perceived online threats. The role of media literacies is of particular importance in this respect, with children and young people requiring the necessary critical and conceptual tools allowing them to deal with, rather than be protected from, the media culture that surrounds them (Hagen and O'Neill, 2009). Moreover, it has been suggested that the association between online safety skills and digital literacy needs to be further explored, as increasing one may also increase the other (Sonck et al., 2011).

According to Buckingham (2007a) the aim of digital literacies is to ensure that young people are able to both understand and participate in the media – which have further been described as vital for both individual life and society and form a key part of digital inclusion (Van Deursen et.al., 2014). This is based on literacies being important for both locating media content and using the available technologies and software, but also in being able to regulate (or self-regulate) access, by being aware of potential risks and using regulatory mechanisms and systems of guidance (Buckingham 2007b).

As Jolls and Thoman (2005) identify, media literacy therefore plays an important role for young people, helping them to acquire an empowering set of “navigational” skills encompassing the ability to:

- Access information from a variety of sources.
- Analyse and explore how messages are constructed.
- Evaluate media’s explicit and implicit messages against one’s own ethical, moral and/or democratic principles.
- Express or create their own messages using a variety of media tools.

As a consequence, digital skills and literacies include active and reactive responses to online content, including both responses to risk and engagement with online opportunities. Therefore, ‘internet literacy plays a key role in mediating online experience and should, therefore, be included in future research on access, use, opportunities and risks online’ (Livingstone and Helsper, 2010, p. 17).

In contrast to the perception of young people being naturally well versed in online skills (the myth of the digital native), young people do not naturally or automatically acquire digital literacies (Livingstone and Haddon et al., 2014). Instead of an individual’s age and year of birth, breadth of use, experience, self-efficacy and education are more important in explaining how people become digital natives (Helsper and Eynon, 2009). Crucially, as it is argued generational gaps are of little importance with respect to digital literacies, ‘collaboration and learning is possible in environments where younger and older generations interact’ (Ibid.). This has an important impact on the role of child online safety education, both with regards to parental mediation and educational policies.

Furthermore, as technologies develop quickly, teaching these skills is becoming more important if young people are to navigate the internet safely and demonstrate the required levels of digital resilience. Similarly, understanding the factors that hinder the uptake of digital skills and literacies is equally important in fostering greater levels of resilience internationally.

Barriers to Resilience

Even though children’s digital literacy skills on the whole are increasing, a number of the creative, informative, interactive and participatory elements of the digital environment are failing to be accessed by a wide range of the global population.

Barriers to media literacy have been argued are often predominantly barriers to access (both access to media opportunities and media consumption) and can range from economic, institutional, social, and personal factors (Buckingham et al., 2005).

This 'digital divide' focuses on the inequalities present in the divisions within and across societies according to those who have access to digital technologies and those that do not (Livingstone and Helsper, 2007). This is important as it has been noted that people who have less access to technology have fewer opportunities to develop their media skills and competencies, are less likely to seek opportunities and as a result are less likely to develop resilience (Buckingham et al., 2005).

Although access is an important determinant of resilience, based on the fact that children's digital access is growing apace, the digital divide can also encompass even well-resourced children who are underusing the opportunities available (Bulger and Livingstone, 2014). This has reframed the debate away from mere availability and access to technology, to the 'trickier question of social and cultural factors that influence use' (Livingstone and Helsper 2007, p. 3). It also raises the question of how to move beyond the provision of access, and how to increase both the scale and quality of opportunities for the broadest possible population (Collier et al., 2014). Moreover, it has been argued these 'untapped opportunities to benefit from the internet are particularly challenging in lower income countries and among socially excluded groups of children' (Bulger and Livingstone, 2013, p.4)

Other factors consequentially play an integral role in either fostering or preventing resilience when online. According to the findings of EU Kids Online (Livingstone and Tink, 2012), children from an educational and economic disadvantage or with parents who rarely used the internet were seen as less resilient. This is based on their likelihood to:

- Take less risk; yet react more negatively to risk.
- Harbour fewer digital skills and literacies
- Refrain from seeking help (communicative coping) from their parents
- Receive less safety information from their parents

Children with a psychological disadvantage were found to have fewer digital skills, and to take more risks (while being vulnerable to risk). Also, children with a social disadvantage were found to be more vulnerable to online bullying.

However, despite these distinctions, it was noted that 'many unknown factors account for children's vulnerability online (Livingstone and Tink, 2012, p.23).

These examples illustrate the difficulty in measuring vulnerability, yet emphasise the role of skills and literacies in the uptake of opportunities, in responding positively to risk and in demonstrating higher levels of digital resilience.

Defining Risk, Harm and Vulnerability

While resilience is fundamental in responding to the wide array of situations the internet can provide, understanding risk, harm and vulnerability is equally essential. Definitions of risk, harm and vulnerability have often been confused with reference to the discourse of child online safety. This is not surprising considering the relationship between risk, harm and vulnerability is complex (Collier et al., 2014). As Bulger and Livingstone (2014) note, this has resulted in risk (e.g. exposure to pornography) and harm (e.g. distorted sexual identity resulting from exposure to pornography) being easily confused. Despite this, risk has been defined as the 'possibility that human actions or events lead to consequences that harm aspects of things that human beings value (Klinke and Renn, 2002, p. 1071). Crucially, therefore, 'risks describe probabilities and not certainties' (Schoon 2006, p. 10).

Moreover, harm is often defined as either physical or mental damage, or material damage, actual or potential ill effect (Livingstone, 2010). This risk harm distinction is important to make, particularly in terms of moving beyond a framework that solely focuses on preventing harm without fully comprehending its relation to risk (and the opportunities risk can create) - resulting in restricting young people's exploration of, and access to the internet.

While it has been argued that harm and vulnerability are implicitly understood, vulnerability has been defined as the susceptibility to physical or emotional injury (Munro, 2011). More importantly, however, vulnerability cannot always be associated with a certain group of individuals based on the fact that:

'...vulnerable children and young people are not a self-contained or static group. Any child/young person may be vulnerable at some time depending on any one, or a combination of, the risks or challenging life events they face' (Cross et al., 2009).

Empowerment: Balancing Opportunities and Risks

While ensuring children and young people are safe when navigating the internet is a key priority for policy makers, educators and parents alike, empowering children to take full advantage of the opportunities the internet provides is also of utmost importance. The opportunities available are wide in scope, ranging from learning, communication, civic participation, creativity, self-expression and entertainment (Livingstone and Helsper, 2010). Moreover, young people are teaching themselves new skills when interacting with online media, including computer programming, amongst others (Prensky, 2008). This 'ladder of opportunities' highlights the progression of online activities, with most children engaging first with basic activities and progressively climbing the ladder to take up the more creative and participatory activities (Livingstone et al., 2011).

The current international policy climate emphasises risk over opportunities, with security being seen as a more fundamental challenge for internet regulation. However, it is widely recognised that online opportunities bring risks with them, while efforts to manage risks can limit children's online opportunities (Bulger and Livingstone, 2013, p. 15). This further reiterates the role of resilience in equipping children with the tools needed to benefit most from the internet, thus mitigating risk through education and awareness without giving away freedom of opportunities.

Using the findings of a UK based survey, it was found that those who took up more opportunities encountered more risks, and vice versa (Livingstone and Helsper, 2010). Contrastingly, some of the countries present in the EU Kids Online report refute this assumption, with respondents from Belgium, Portugal and the UK 'benefitting from more online activities without an equivalent increase in risk' (Livingstone, 2014b, p. 2). This both reinforces the perception that online habits are peculiar to cultural contexts alongside the need for further empirical evidence within this area to add to the current body of research.

Challenges for Internet Governance

Striking a balance between security and freedom is the most contentious aspect of internet governance internationally, particularly based on the fact that the online environment presents a challenge in terms of responsibility and authority related to rights and risk assessment (Bulger and Livingstone, 2013).

At the International level, the UN Convention on the Rights of the Child (1989) acts as a guideline for safeguarding children's rights online (with signatories required to adopt appropriate measures), particularly in terms of facilitating the exercise of their right to express an opinion, promote citizen participation and to 'provide a conduit for their freedoms of expression and information' (UNICEF, 2014, p. 7).

Moreover, there are a number of international initiatives linking stakeholders for international co-operation on internet policy, including the ITU's Child Online Protection (COP) Initiative, and the Internet Governance Forum (IGF), amongst others. This is accompanied by a multitude of child welfare organisations (including Childnet International, The European Child Safety Online NGO Network and the Family Online Safety Institute) (OECD, 2012).

The perceived benefits of including internet safety and digital skills in school curricula are vast. Inclusion into school curricula is expected to increase awareness of the risks that kids may encounter and foster a more responsible use of the web. In addition, a more focused effort towards teaching digital literacy is legitimately expected to widen the array of instrumental actions used to cope with online risk and harm.

Somewhat surprisingly, according to the survey's results, children learn the most about internet safety from their friends (52%), followed by parents (43%) and at school (39%). However, this view is contrasted with their preference for where to seek advice on internet safety as only 28% of them list friends as their first preference, and instead seek advice from a parent or guardian (37%). When learning about internet safety at school is contrasted with different measures of resilience some interesting results emerge. Namely, children who have mostly learned how to surf the web at school display higher resilience scores for the instrumental action and disengagement strategies dimensions.

This reinforces the view that school is the best place to learn digital safety and that the inclusion of digital literacy in school curriculum would augment its relevance for kids.

Regional Frameworks

At the regional level both the European Union and the Council of Europe have developed policy frameworks protecting children online, ranging from Directives combating the exploitation of children through ICT usage (UNICEF, 2011) to harmonised legislation pertaining to child protection online. Moreover, through the Safer Internet Programme (SIP) the EU assumes 'a regional lead in stimulating policy making and implementation as well as co-operation between its member states' (OECD, 2012, p. 60). Despite regional instruments having specific application within the region they are developed in, they often act as a benchmark for other countries to adopt and 'in some instances allow ratification by States from outside the region' (UNICEF, 2011, p. 10).

National Level

Governments worldwide are developing national frameworks for the protection of children online, in line with article 3 of the UN Convention (OECD, 2012). However, varying approaches are adopted, with some countries opting for a 'more holistic policy framework in which national priorities are defined with a view to enhancing policy coherence' (e.g. the EU within its competences, Australia, Canada and the United Kingdom) (OECD, 2012, p. 47).

The Australian Government has implemented a number of strategies for promoting online safety, of which the Cyber smart Programme is one of its flagship initiatives. Managed by the Australian Communications and Media Authority (ACMA) and targeted towards young people, parents and teachers, the programme aims to support and encourage young people to productively engage in the digital economy and protect themselves 'by demonstrating positive, ethical, and balanced online behaviour' (UNESCO 2014, p. 14). Alongside this, the 2008 Cyber safety Plan promotes cyber-safety education, law enforcement and awareness-raising activities (OECD, 2012). Similarly, in Japan the issue of child online protection has been taken up at cabinet level, with mandatory filters present on mobile phones for users under 18 (unless parents opt out), and the regulation of child-inappropriate content under their 2008 Act on Development of an Environment that Provides Safe and Secure Internet use for Young People (Ibid.). These regulation have significantly reduced the amount of inappropriate content online as only 28% of Japanese kids reported to have seen age inappropriate content compared to the maximum registered in Indonesia (53%)

A number of internet related initiatives in Korea have been introduced, including the Communications Commission Act, the Information Protection Act and the Child Protection Act, amongst others. These are aimed at promoting healthy internet usage, cyber ethics, and online safety including content rating systems and filtering software (OECD, 2012). Indonesia has also implemented the blocking and filtering of content (predominantly pornographic) and are in collaboration with UNICEF in designing a National Plan of Action on Safe Media, including the strengthening of policies and conducting public awareness campaigns (UNESCO, 2014). Content filters policies aimed at tackling pornography resulted in a low exposure to age inappropriate content in Korea (39%), whereas the Indonesian filtering policy (53%) does not seem to fully address the issue.

The Taiwanese government implemented the Protection of Children and Youths Welfare and Rights Act, in which several measures aim at promoting online safety for minors. Thus, Internet platform providers have to establish protective measures to prevent children and youth from seeing harmful Internet content, and no one is allowed to spread or broadcast contents through Internet that will be harmful to children and youth's mental health. Alongside these legal barriers, a private initiative deserves to be underlined: Microsoft Taiwan is collaborating with the international non-governmental organisation ECPAT Taiwan (End Child Prostitution, Child Pornography And Trafficking of Children for Sexual Purposes) to fight for cyber-safety for children. For example, a Microsoft-ECPAT initiative titled "4G" (Time Guardian, History Guardian, Web Guardian and Rating Guardian) enables parents to use free Microsoft tools to ensure a safe web browsing experience for their children. They also developed a set of guidelines in order to help parents deal with their children's online security.

Risk vs. Opportunity: Instruments to Strike the Right Balance

Content Blocking Filters

With the view of minimising access to inappropriate content, all of the surveyed countries have implemented technical measures. Among these, content blocking software (e.g. filters) is particularly widespread in Indonesia.

The perceived benefits of content blocking lies in reducing the amount of illegal content online (i.e. depictions of child sexual exploitation, bestiality, etc.) and reduce the amount of unsuitable content. Their effectiveness however depends on percentages of false negatives and false positives, i.e. the rate of under blocking (allowing undesired content which should be blocked) and the rate of over blocking (not allowing content which is “good” for children) (OECD, 2012).

Similarly, the effectiveness of content blocking filters may also hinge on the level on which these filters are implemented i.e. at i) network level (e.g. Internet Service Provider network or local area networks); ii) server-level (e.g. social network site or search engine) (ibid.)

Results on child strategies in dealing with online content risk may provide an additional perspective to the filters’ effectiveness debate. According to these, children display a relatively high take up of technical strategies minimising their access to unsuitable content. For example 61% of children report having installed filters on their own, while 53% of them are likely to use child friendly search engines. Moreover, the most common reaction to unwanted disturbing content is the immediate closing of the page as reported by 59% of children. All in all, these results support the view that the majority of children effectively self-regulate when facing disturbing content.

School and Education

The role of formal education in fostering awareness and promoting safe internet use cannot be underestimated. While this has been widely recognised as a key policy priority by experts and researchers (UNESCO 2014; UNICEF 2012; Livingstone et al. 2013) there is little evidence of curricular adjustments in this sense in the surveyed countries. With the exception of Korea, where the Korean Internet and Security agency has implemented internet literacy and ethics classes, no other country seems to have developed such policies (UNESCO, 2014).

The perceived benefits of including internet safety and digital skills in school curricula are vast. Inclusion into school curricula is expected to increase awareness of the risks that kids may encounter and foster a more responsible use of the web. In addition, a more focused effort towards teaching digital literacy is legitimately expected to widen the array of instrumental actions used to cope with online risk and harm.

According to the survey’s results, school is the place where most of the kids learn about internet safety (64%). However, this view is contrasted with their opinion on who they reach out to when seeking advice on internet safety as only 17% of them list school as a valid option. When learning about internet safety at school is contrasted with different measures of resilience some interesting results emerge. Namely, children who have mostly learned how to surf the web at school display higher resilience scores for the instrumental action and disengagement strategies dimensions.

This reinforces the view that school is the best place to learn digital safety and that the inclusion of digital literacy in school curriculum would augment its relevance for kids.

Hotlines and Reporting Mechanisms

The introduction of more widespread reporting mechanisms, including hotlines, report abuse functions, and online supports to pre-empt abusive situations (UNICEF, 2011) have been suggested are effective means of enhancing resilience. Moreover, some social networking sites already have these kinds of options whereby a young person can be put in touch with law enforcement agencies when feeling vulnerable or threatened.

However, according to the results of this study, using reporting mechanisms or hotlines as a communicative strategy is the one of the least frequently adopted mechanisms internationally across the entire range of online risks outlined in the preceding analysis.

This includes only 3% of respondents adopting this strategy in response to disturbing messages, 8% for the misuse of personal information, and 9% for instances of cyber-bullying. More research is therefore needed in order to determine the effectiveness of these tools and how their use can be spread.

Extra-Curricular Learning

Improving the quality and accessibility of online skills education is one of the key global policy initiatives for fostering greater levels of resilience amongst young people. The perceived benefits of this are widespread, ranging from the uptake of more online opportunities to a deeper critical understanding of online content and the risks that are present.

Based on this it has been noted that enhancing extra-curricular learning activities and through the involvement of educational providers, industry, child welfare and other organisations in expanding digital literacy programmes, children would be able to increase their online competences and benefit from a wider range of opportunities (Livingstone and Helsper, 2010). Moreover, this has an important role to play in linking children with internet stakeholders and in listening to their experiences and insights (Byron, 2008).

The success of extra-curricular online safety education is further reinforced from the results of this study, with outside learning being the most effective path towards higher levels of confrontational reactive strategies in response to risk online.

Policy Recommendations

Based on the existing policy options and in light of both the theoretical discussion of safety concerns and the results of the survey, this study recommends a stronger balance between security and freedom with a focus on initiatives fostering child online resilience through access and experience instead of technical and legislative restrictions.

In particular, this study recommends to:

- Promote the inclusion of enhanced digital literacy and internet safety education into school curricula from early childhood education and care, and to ensure the provision of ICT training for teachers and educators.

- Foster extra-curricular activities aimed at promoting responsible and mutually respectful internet use for young people.
- Improve and promote the existing hotline support services as a more reliable means to convey child concerns and to report problems.
- Minimise the impact of over-reaching content filters that might undermine a child's access to information and restrict a child's ability to learn, explore, and build resilience through active engagement with the online world.

Conclusion

The preceding analysis of child online safety has aimed to shed light on the often misconceived relationship between the risks and opportunities faced by children. Taking into account the perspectives of both child protection advocates and advocates of freedom of information and expression, the preceding analysis focussed on the role of digital resilience in equipping children with the navigational tools required to stay safe when online, while also maximising the opportunities the internet provides.

Moreover, based on the lack of country specific and region-wide research internationally, this study was focussed on adding to the existing body of empirical data on child online resilience; investigating the online habits of 9-18 year old children and young people in Australia, Japan, Korea, Taiwan, and Indonesia.

By focussing on the role of media skills and competencies in responding to risks online, it was found that young people with both high levels of internet literacy and a critical awareness of online content were able to effectively self-regulate their media usage. Furthermore, this had a positive impact on the young person's digital resilience, and therefore in his/her ability to adapt to and avoid stressful situations online. The results also identified children as on the whole being aware of the 'think before you post' principle, despite certain country level variations being present in relation to perception of risk. Taking into the account the variety of reactive strategies employed by young people when faced with online risk, it was found that the length of time spent online, a young person's psychological makeup, and where they learn their online safety skills play an important part in the types of reactive strategies to risk adopted, and as result, in their level of digital resilience.

Based on the importance of skills and competencies in relation to both understanding online content and in being able to respond effectively to risk, the findings of this research reiterated the need to bring effective media literacy into education and policy, with a key goal in emphasising the role of teachers as facilitators of creativity, innovation and resilience (Donoso and Lievens, 2014). Moreover, the evidence suggests that online protection is often best realised by ensuring young people have access to the online world, and gain meaningful experiences through a positive engagement with online content. This is facilitated best by promoting online participation, and refraining from the excessive restrictions to online content.

Additionally, the positive correlation between exposure to risk and the ability to employ effective coping strategies reiterates the suggestion that increasing a young person's engagement with the online world fosters higher levels of digital resilience.

Accompanying this, it has become clear that creating the right international environment for fostering digital resilience amongst children and young people requires a multifaceted approach, requiring the efforts of families, teachers, policy-makers, industry and academia alike (Linnington et al., 2014).

References

- Bartley, M. (2006). *Capability and Resilience: Beating the Odds*. UCL Department of Epidemiology and Public Health.
- Becker, B. Cicchetti, D and Luthat, S. S (2000) 'The Construct of Resilience: A Critical Evaluation and Guidelines for Future Work' *Child Dev.* 2000; 71(3): 543-562
- Buckingham, D (2007b) 'Digital Media Literacies: rethinking media education in the age of the Internet' *Research in Comparative and International Education*, Volume 2, Number 1.
- Buckingham, D. (2006). *Defining Digital Literacy*. *District Dispatch*, 263–276. Retrieved from <http://www.districtdispatch.org/2012/04/defining-digital-literacy/>
- Buckingham, D. (2007a) *Beyond Technology: Children's Learning in the Age of Digital Culture*, Oxford: Polity Press.
- Buckingham, D., Banaji, S., Burn, A., and Carr, D. (2005). *The media literacy of children and young people*. London. Retrieved from [http://www.aeforum.org/aeforum.nsf/0/f49f4f9ae98cdc9b80256fb70060b61c/\\$FILE/DB05medialiteracyOfcom.pdf](http://www.aeforum.org/aeforum.nsf/0/f49f4f9ae98cdc9b80256fb70060b61c/$FILE/DB05medialiteracyOfcom.pdf)
- Bulger, E. M and Livingstone, S (2013) 'A Global Agenda for Children's Rights in the Digital Age, Recommendations for Developing UNICEF's Research Strategy' UNICEF Office of Research – Innocenti.
- Byron, T. (2008) 'Safer children in a Digital World: The Report of the Byron Review' *Byron Review – Children and New Technology*.
- Collier, A. Forrest-Lawrence, P and Third, A. (2014) 'Addressing the Cyber Safety Challenge: From Risk to Resilience' University of Western Sydney Institute for Culture and Society.
- Cross, E.J., Richardson, B. Douglas, T. and Vonkaenel-Flatt, J. (2009) *Virtual violence: protecting children from cyberbullying*. London: Beatbullying.
- Davies, T (2011) 'Rethinking Responses to Children and Young People's Online Lives' EU Kids Online 2 Final Conference – September.
- Donoso, V and Lievens, E (2014) 'Bringing Media Literacy into Education and Policy' LSE Media Policy Project Blog. Available at: <http://blogs.lse.ac.uk/mediapolicyproject/2014/05/27/bringing-media-literacy-into-education-and-policy/>
- Donoso, V, d'Heanens, L and Vandoninck, S (2013) 'How to cope and build online resilience?' *EU Kids Online*.
- Gasser, U., Maclay, C., and Palfrey, J (2010) 'Working Towards a Deeper Understanding of digital Safety for Children and Young People in Developing Nations', Harvard Law School Public Law & Legal Theory Working Paper Series, 10-36.
- Hasebrink, U., Livingstone, S., and Haddon, L. (2008). *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. London: EU Kids Online (Deliverable 3.2.)
- Helsper, Ellen and Eynon, Rebecca (2009) 'Digital natives: where is the evidence?' *British educational research journal* pp. 1-18.
- Hills, M., Nash, V., Powell, A. (2010). *Child Protection and Freedom of Expression Online*. Oxford Internet Institute Forum Discussion Paper No.17.
- Klinke, A and Renn, O. (2002) 'A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies' *Risk Analysis*, Vol.22, No.6.
- Livingstone, S (2014b) 'Maximising the opportunities for kids online – where are we?' LSE Media Policy Blog. Available at: <http://blogs.lse.ac.uk/mediapolicyproject/2014/12/02/maximising-the-opportunities-for-kids-online-where-are-we/>
- Livingstone, S and Helsper, E (2010) *Balancing opportunities and risks in teenager's use of the internet: the role of online skills and internet self-efficacy*. *New Media and Society*, 12 (2). Pp. 309-329. Available at: <http://eprints.lse.ac.uk/35373/>
- Livingstone, S and Palmer, T (2012) *Identifying vulnerable children online and what strategies can help them*. UK Safer Internet Centre, London, UK. Available at: <http://eprints.lse.ac.uk/44222/>
- Livingstone, S. (2010) 'e-Youth: (future) policy implications: reflections on online risk, harm and vulnerability' Originally presented at e-Youth: balancing opportunities and risks, 27-28 May 2010, UCSIA & MIOS University of Antwerp, Antwerp, Belgium.
- Livingstone, S. (2013) 'Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy' *Zer Vol.18 – NOM*. 35 PP.13-28
- Gasser, U., Maclay, C., and Palfrey, J (2010) 'Working Towards a Deeper Understanding of digital Safety for Children and Young People in Developing Nations', Harvard Law School Public Law & Legal Theory Working Paper Series, 10-36.
- Hasebrink, U., Livingstone, S., and Haddon, L. (2008). *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. London: EU Kids Online (Deliverable 3.2.)
- Helsper, Ellen and Eynon, Rebecca (2009) 'Digital natives: where is the evidence?' *British educational research journal* pp. 1-18.
- Hills, M., Nash, V., Powell, A. (2010). *Child Protection and Freedom of Expression Online*. Oxford Internet Institute Forum Discussion Paper No.17.
- Klinke, A and Renn, O. (2002) 'A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies' *Risk Analysis*, Vol.22, No.6.

- Livingstone, S., Mishkin, A., Przybylski, K. A. and Shotbolt, V. (2014) 'A Shared Responsibility, Building Children's Online Resilience' The Oxford Internet Institute, Virgin Media and The Parent Zone.
- Livingstone, S. (2014b) 'Maximising the opportunities for kids online – where are we? LSE Media Policy Blog. Available at: <http://blogs.lse.ac.uk/mediapolicyproject/2014/12/02/maximising-the-opportunities-for-kids-online-where-are-we/>
- Livingstone, S. and Helsper, E. (2010) Balancing opportunities and risks in teenager's use of the internet: the role of online skills and internet self-efficacy. *New Media and Society*, 12 (2). Pp. 309-329. Available at: <http://eprints.lse.ac.uk/35373/>
- Livingstone, S. and Palmer, T. (2012) Identifying vulnerable children online and what strategies can help them. UK Safer Internet Centre, London, UK. Available at: <http://eprints.lse.ac.uk/44222/>
- Livingstone, S. (2010) 'e-Youth: (future) policy implications: reflections on online risk, harm and vulnerability' Originally presented at e-Youth: balancing opportunities and risks, 27-28 May 2010, UCSIA & MIOS University of Antwerp, Antwerp, Belgium.
- Livingstone, S. (2013) 'Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy' *Zer Vol.18 – NOM*. 35 PP.13-28
- Livingstone, S. (2014b) 'Digital Media and Children's Rights', LSE Media Policy Project blog. <http://blogs.lse.ac.uk/mediapolicyproject/2014/09/12/sonia-livingstone-digital-media-and-childrens-rights/>. Accessed 26.05.2015.
- Livingstone, S., Bulger, M. (2014) 'A Global Research Agenda for Children's Rights in the Digital Age' *Journal of Children and Media*, DOI: 10.1080/17482798.2014.961496
- Livingstone, S., Haddon, L., Görzig, A. and Ólafsson, K. (2011) EU kids online: final report. EU Kids Online, London School of Economics & Political Science, London, UK. Available at: <http://eprints.lse.ac.uk/39351/>
- Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G. and Ólafsson, K. (2014) 'Net Children Go Mobile, The UK report. London: London School of Economics and Political Science.
- Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full findings. LSE, London: EU Kids Online. Available at <http://eprints.lse.ac.uk/33731/>
- Livingstone, Sonia and Helsper, Ellen (2007) Gradations in digital inclusion: children, young people and the digital divide. *New media & society*, 9 (4). pp. 671-696.
- Ministry of the Interior of the Republic of China (Taiwan), The Protection of Children and Youths Welfare and Rights Act, art 43, 46, 49.
- Munro, R. E. (2011) 'The protection of children online: a brief scoping review to identify vulnerable groups' *Childhood Wellbeing Research Centre*.
- OECD (2012) 'The Protection of Children Online, Recommendations of the OECD Council' Report on Risks Faced by Children Online and Policies to Protect Them.
- Prensky, M. (2008). Students as designers and creators of educational computer games: Who else? *British Journal of Educational Technology*, 39(6), 1004– 1019. doi:10.1111/j.1467-8535.2008.00823_2.x
- Sonck, N., Livingstone, S., Kuiper, E., and de Haan, J. (2011) Digital Literacy & Safety Skills. EU Kids Online, Retrieved from: [http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%2011%20\(2009-11\)/EUKidsOnlineReports/DigitalSkillsShortReport.pdf](http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%2011%20(2009-11)/EUKidsOnlineReports/DigitalSkillsShortReport.pdf)
- Thoman, E. (2005) 'Literacy for the 21st Century, An Overview & Orientation Guide To Media Literacy Education' Center for Media Literacy.
- UNESCO (2014) 'Fostering Digital Citizenship through Safe and Responsible Use of ICT, a review of current status in Asia and the Pacific as of December 2014' APEID-ICT in Education UNESCO Regional Bureau of Education.
- UNICEF (2014) 'Challenges: Children's rights in the digital age' Newsletter on progress towards the Millennium Development Goals from a child rights perspective, Number 18, September 2014.
- UNICEF. (2011) 'Child Safety Online, Global challenges and strategies' UNICEF Innocenti Research Centre
- Van Deursen, A.J.A.M., Helsper, E.J. and Eynon, R. (2014). Measuring Digital Skills. From Digital Skills to Tangible Outcomes project report. Available at: www.oii.ox.ac.uk/research/projects/?id=112

Appendix A: Resilience scores

Behavioural preventive		Disengagement resilience		Cognitive scores		
					mean	ideal
Australia	2.66126	Taiwan	1.82418	Taiwan	2.21	73.5%
Indonesia	2.62264	Australia	1.65517	Australia	2.16	71.9%
Taiwan	2.58608	APAC	1.51988	APAC	1.98	66.1%
APAC	2.44359	Korea	1.41333	Indonesia	1.97	65.7%
Korea	2.19216	Japan	1.38444	Korea	1.80	60.1%
Japan	2.15560	Indonesia	1.31774	Japan	1.77	59.0%
Instrumental preventive		Instrumental coping		Instrumental scores		
					mean	ideal
Indonesia	2.26250	Australia	1.62899	Indonesia	1.82	60.8%
Taiwan	2.10188	Indonesia	1.38593	Australia	1.82	60.8%
Australia	2.01876	Taiwan	1.37995	Taiwan	1.74	58.0%
APAC	1.93587	APAC	1.28814	APAC	1.61	53.7%
South	1.68333	Korea	1.23636	South	1.46	48.7%
Japan	1.60223	Japan	0.82594	Japan	1.21	40.5%
Confrontational resilience		Communicative resilience		Communicative scores		
					mean	ideal
Indonesia	1.28792	Australia	1.05475	Indonesia	1.06	35.4%
Taiwan	0.91505	Taiwan	0.87111	Australia	0.98	32.7%
Australia	0.90525	Indonesia	0.83360	Taiwan	0.89	29.8%
APAC	0.87430	APAC	0.75824	APAC	0.82	27.2%
Korea	0.83194	Korea	0.58323	Korea	0.71	23.6%
Japan	0.42817	Japan	0.45747	Japan	0.44	14.8%

APPENDIX B: Determinants of Resilience - Descriptive Analysis

Summary

As digital resilience is affected by a number of factors, the following section analyses the results with reference to children’s critical awareness of online content, where they are most likely to learn digital skills and their level of digital competence. According to the results:

More prevalent differences are present at the country level when compared to the age group level.

No significant difference exists between young children and older teens in terms of their awareness of risk and critical understanding of online content. Significant variations are present when the results from Japan are taken into account (particularly in terms of confidence in online skills).

Country level differences exist for how children perceive online friends, and where they are most likely to learn internet safety.

Media Skills and Digital Literacies

International Analysis

The international results illustrate a high level of competence across countries in finding effective keywords for content searching online, with 48% stating they are ‘very confident’ in this skill (net confidence 86%). This is closely followed by children having a high net confidence in changing their social media settings (78%) and knowing when the information they retrieve is correct (76%). However, confidence in the ability to use a virtual private network (VPN) to avoid regional blocks on online content is low with a 57% net not confident rating.

Table 1. Digital Skills/Competencies – International level

	All countries							
	Block junk email or spam	Delete history` records on web browsers	Change settings to use a web browser in privacy mode	Set filters or content controls for certain websites	Use a VPN to circumvent geo restrictions	Find good keywords	Know when the information I retrieve is correct	Post comments on blogs or websites
Very Confident	42%	43%	33%	28%	19%	48%	36%	34%
Fairly Confident	31%	29%	32%	33%	24%	38%	40%	34%
Not That Confident	19%	19%	22%	26%	30%	10%	19%	21%
Not At All Confident	8%	9%	12%	13%	27%	4%	5%	11%

Country Level Analysis

While the country level variations on the whole are quite similar, some substantial differences in perceived online skills and competencies exist between countries. Indonesia and Japan display the most polarised perceptions of online skills, with Japanese children having a net lack of confidence in every skill surveyed (with 74% lacking confidence in knowing when online information is correct). For instance, while 92% of young Indonesians feel confident with finding good keywords, only 48% of the Japanese children surveyed answered to be confident in this case.

Contrastingly, children in Indonesia display high levels of confidence in all skills, including 29% being very confident in using a VPN (only 19% internationally).

Children from Indonesia are also the most confident in their self-expression abilities with 79% being confident in posting a comment on a blog or website (compared to only 31% in Japan and 61% in Korea).

Table 2. Digital Skills/ Competencies – Country Level

	Use a VPN to circumvent geo-localisation restrictions				
	Indonesia	Japan	Korea	Australia	Taiwan
Very Confident	29%	7%	9%	7%	23%
Fairly Confident	36%	10%	22%	17%	35%
Not That Confident	29%	37%	45%	33%	31%
Not At All Confident	7%	45%	24%	43%	10%
	Post comments on blogs or websites				
	Indonesia	Japan	Korea	Australia	Taiwan
Very Confident	39%	10%	15%	30%	28%
Fairly Confident	40%	21%	47%	37%	49%
Not That Confident	19%	43%	30%	22%	20%
Not At All Confident	2%	26%	9%	12%	2%

Education and Learning Pathways

Country Level Analysis

Where children seek advice for internet safety demonstrates some interesting country variations. Children in Indonesia (14%), Taiwan and Japan (17% in both countries) show little interest in learning from friends when compared to 33% in Korea. Taiwanese and Japanese children are also the most likely to seek help from a parent or guardian (47% and 66% respectively).

Table 3. Preferred Learning Pathways

	All countries	Indonesia	Japan	Korea	Australia	Taiwan
From your parent(s)/guardian(s)	42%	43%	66%	32%	41%	47%
From your friends	28%	14%	17%	33%	21%	17%
From your teachers at school/lecturers	16%	28%	6%	16%	21%	24%
From lessons outside of school/college	6%	12%	5%	11%	3%	9%
From brothers/sisters	4%	2%	4%	4%	8%	3%

Awareness and Critical Thinking

The results of the survey from the international sample identified young people as on the whole being critically aware of both online content and the potential for risk. Overall the highest scores relate to the ability of distinguishing between something funny and friendly and something wrong (45%) and thinking carefully before what action to take online (44%).

Table 4. Awareness and Critical Thinking – International Sample

	I can usually tell when something is funny and friendly and when something might be wrong or bad	Friends you only know online are different to real friends	I can easily tell when something I see online is false or wrong	I usually think carefully about things before deciding what I should do	I can usually tell when something looks suspicious or risky
Very true	45%	43%	27%	44%	37%
A bit true/Somewhat true	50%	37%	57%	46%	51%
Not true	5%	19%	15%	10%	12%

Of particular interest is the response on the question to whether children perceived online friends separately from offline. In this case, the results display notable country differences.

As table 5 demonstrates, children in Taiwan have the highest belief in a distinction between online and offline friends with a 96% net true rating. In contrast to this, children in Indonesia (31%) and Korea (29%) see no difference in the two types of friend.

Table 5. Awareness and Critical Thinking – International Sample

	All countries	Indonesia	Japan	Korea	Australia	Taiwan
Very true	42%	38%	44%	34%	45%	55%
A bit true/Somewhat true	37%	32%	38%	37%	40%	41%
Not true	21%	31%	18%	29%	15%	4%

Table 24. Confrontational Resilience and Self-Efficacy

Confrontational	Mean	Std. Dev.
Self-Efficacy		
Low	0.7055	.599
Medium	0.8998	.714
High	1.1845	.846

Correlation Analysis

Resilience Scores and Personality Traits

The relationship between personality traits and resilience to online risk has always been present in the debates on online resilience. The aim of this section is therefore to confront findings of the existing literature with the specificities of the Asia Pacific region.

The ThinkYoung survey has therefore attempted to capture certain personality traits that might be good predictors of online resilience and classified according to the following categorisation: self-discipline, self-efficacy, anxiety and sociality.

Self-Discipline

The notion of self-discipline has been captured by the likelihood of being very often well behaved and of doing what is told or expected. Self-discipline is expected to be positively associated with preventive and reactive resilience strategies.

The results of a one-way ANOVA analysis illustrate a clear and significant positive association between self-discipline and reactive strategies. Children who report to be more disciplined are more likely to adopt instrumental actions, and confrontational and communicative strategies. The results are significant at a 0.01 confidence level as illustrated by the F-test. The association between discipline and disengagement strategies is less clear as it is found to be positive but not significant.

Self-Efficacy

Self-efficacy is captured by the ability to stick to and achieve one's goals, as well as the confidence in dealing with new things. Self-efficacy is also expected to be associated with a higher degree of resilience as being able to deal with unexpected circumstances is central to the reactive resilience definition in this study.

Not surprisingly, children displaying higher levels of self-efficacy also score higher in three out of four categories of reactive resilience. Namely, the positive association is significant for the F-test with regard to instrumental actions, confrontational and communicative strategies.

Anxiety

With the view of analysing a broad range of positive and negative personality traits, the study has also investigated how anxiety translates into resilience. In line with the psychological literature, the anxiety trait has been captured by its symptoms: worrying a lot and having headaches or stomach aches.

Anxiety is thus expected to negatively correlate against different dimensions of resilience as more anxious children are believed to be more affected by trauma.

Contrary to the expectations and results from previous literature (Donoso et al. 2013) the analysis of variance reveals that children displaying higher levels of anxiety are more likely to adopt 3 out of 4 reactive resilience strategies identified in the study. More specifically, more anxious children are more likely to adopt instrumental actions, confrontational and disengagement strategies.

Table 25. Anxiety and Behavioural Preventive Strategies

Confrontational		
Self-Efficacy	Mean	Std. Dev.
Low	0.7055	.599
Medium	0.8998	.714
High	1.1845	.846

Sociability

The ability or inability of entertaining positive social relations is also one of the personality traits that might come into play when analysing resilience. To capture this aspect the study asked children to report whether they spend a lot of time on their own or whether they have been troublesome and played up with other children.

As some reactive strategies rely on the support of other people (friends, family and teachers) it is expected that less sociable children would be less inclined to adopt communicative and confrontational strategies.

The results show that this is partially true. If on the one hand less sociable children are less likely to undertake communicative strategies, on the other hand they are still more likely to confront their stressor or aggressor.

Unsurprisingly, less sociable children are much more likely to adopt instrumental action and disengagement strategies.

Resilience Score and Type of Internet Usage

The following section provides an overview on the relationship between different types of internet usage and resilience measured by preventive and reactive strategies.

The survey asked children what their main activities for which they were often visiting websites were and how these could in turn influence resilience behaviours. The activities have been grouped into three categories: leisure, educational and social. The results of different correlations are illustrated below.

Educational Activities

The use of internet for educational purposes has been captured by all the instances where children reported to use the internet to learn about something, either related to school activities or to research for information and news.

When contrasted with the measures of resilience identified in this study, use of internet for educational purposes was found to be positively correlated with resilience. More specifically, the results are significant for each of the proposed reactive strategies and, most remarkably, in the case of instrumental action and disengagement strategies, as illustrated in the table below.

Table 26. Instrumental Actions and Use of Internet for Educational Purposes

Instrumental actions		
Educational	Mean	Std. Dev.
0	0.9397	.659
Low	1.2744	.715
Medium	1.4726	.746
High	1.6729	.792

The analysis of the association between measures of digital resilience and use of internet for social or leisure purposes yields very similar results where both types of internet usage are positively associated with resilience.

The explanation of these results is likely to come from the positive association between frequency of internet usage and resilience that has been already echoed in the resilience literature and finds confirmation in this data.

However, when restricting the analysis to the group of those who access internet sporadically results do change. Namely, the positive association is no longer significant and, in some instances, becomes a negative one as in the case of communicative resilience strategies and the usage of internet for social purposes. This result suggests that lower levels of internet access combined with a use of internet for social networking purposes leads to lower levels of resilience.

Resilience Scores, Awareness and Critical Thinking

The notion of digital resilience is very much entrenched with awareness on the peculiarities of the web and the ability of thinking critically about its content. As a result, the study asked children a series of questions to detect their competency level along these dimensions and thus assess their influence on resilience.

Awareness of internet risks is thus associated with the ability to distinguish between online and offline friendships, whereas critical thinking is captured by the extent to which children understand whether something is true or false or differentiate between something that is funny and friendly vs. something that is meant to harm.

Intuitively and in line with previous literature on resilience, the association between resilience and awareness and critical thinking is expected to be positive. In light of this expectation, this study has explored a few correlations to test the hypotheses.

Awareness

The analysis of correlation between awareness and measures of reactive resilience shows mixed results. As an illustration, the likelihood of adopting communicative strategies increases when awareness moves from medium to high and decreases in the move from low to medium levels. Moreover, the adoption of instrumental actions shows no correlation with different degrees of awareness.

The correlation with measures of preventive resilience shows similar unclear patterns with an increase in the adoption of preventive strategies from medium to high levels and a decrease from low to medium levels.

Table 27 Communicative Strategies and Awareness of Online Risks

Online vs. offline friends	Communicative strategies	
	<i>Mean</i>	<i>Std. Dev.</i>
High	0.8291	.796
Medium	0.7364	.781
Low	0.7900	.809

Critical Thinking

The association between critical thinking, identified as the ability to understand whether something is true or false, and different measures of resilience appear to be positive. The results are positive and significant for three out of four reactive strategies including, communicative, instrumental and confrontational actions.

Similarly, measures of preventive resilience are found to be positively correlated with critical thinking abilities, as illustrated in the table below.

Table 28. Technical preventive strategies and Critical Thinking.

True vs. false content	Technical prevention	
	<i>Mean</i>	<i>Std. Dev.</i>
High	2.2867	.543
Medium	1.9225	.595
Low	1.3645	.714

Learning Paths to Safe Internet Use

Children report to have learned how to safely navigate the internet from a variety of sources. The most widespread are parental education, equally followed by formal education and peer learning (e.g. learning from their friends). For the purposes of this study it seems interesting to evaluate where children learn how to navigate the internet has an influence on digital resilience. As a result, correlation analysis between learning paths to safe internet use and resilience strategies has been performed.

The analysis of reactive strategies shows some interesting patterns where formal education, peer learning, extra-curricular and parental education alternate as the best option associated with certain reactive strategies.

Parental Education

Parental education ranks first as a learning path leading to higher levels of communicative strategies, closely followed by peer learning as illustrated in the table below. The result doesn't appear particularly surprising as it is likely that children who have learned how to navigate the internet from their parents or peers will be more likely to ask them for advice when facing risky situations.

Table 29 Learning Paths and Communicative Strategies

Communicative strategies		
	Mean	Std. Dev.
Parental education	0.9168	.800
Peer learning	0.7740	.764
School	0.6782	.733
Extra-curricular courses	0.5793	.736

Formal Education and Peer Learning

Peer learning and schools can be identified as leading learning paths for the adoption of more instrumental actions and disengagement strategies. Across these two measures of reactive resilience children who have learned at school and with their friends display higher levels than their peers who have learned about internet safety through extra-curricular activities and from their parents.

Table 30. Learning Paths, Disengagement Strategies and Instrumental Actions.

Disengagement strategies			Instrumental actions	
	Mean	Std. Dev.	Mean	Std. Dev.
Peer learning	1.417	.968	1.4238	.763
School	1.4055	.985	1.4038	.734
Parental education	1.1604	.989	1.2619	.662
Extra-curricular courses	1.0983	.910	1.157	.711

Group Learning

Lastly and somewhat surprisingly, extra-curricular learning appears to be the most effective path leading towards higher levels of the adoption of confrontational strategies. An explanation of this result may hinge on the group dynamics that are created through school and extra-curricular activities, where children may confront more openly about those issues with their peers. In this case awareness of issues such as cyber-bullying would lead to higher degrees of confrontation and resolve the problems more quickly.

APPENDIX C: Tables in the Report

Table 1. Instrumental Strategies–International level

	Use child friendly search engines (e.g. Kidrex, Google safeKids, Junior etc.)	Have filters and software on that protects me from unwanted content (e.g. adblock) or contacts	Make my profile unavailable to the general public	Modify privacy settings to keep me away from unwanted contacts	Turn off programmes that I consider risky	Use a secondary account for spam and other emails I don't want	Use complicated, safe passwords (with a mix of capital letters, special characters and numbers)	Keep my passwords completely secret from anyone
Very likely	24%	28%	31%	33%	39%	19%	34%	52%
Fairly likely	29%	33%	39%	37%	37%	32%	38%	33%
Not that likely	24%	20%	18%	16%	14%	24%	18%	8%
Not at all likely	12%	6%	6%	4%	3%	12%	4%	3%
Don't Know	12%	14%	7%	10%	8%	14%	6%	4%
NET: Likely	53%	61%	69%	70%	76%	51%	72%	85%
NET: Not likely	36%	25%	24%	20%	17%	35%	22%	11%

Table 2. Children Using Child-Friendly Search Engines

	All countries	Indonesia	Japan	South Korea	Australia	Taiwan
Very likely	24%	52%	10%	15%	21%	20%
Fairly likely	29%	29%	22%	27%	23%	41%
Not that likely	24%	11%	33%	28%	25%	25%
Not at all likely	12%	4%	15%	13%	25%	4%
Don't Know	12%	4%	20%	18%	7%	10%

Table 3. Frequency of Internet Usage and Preventive Instruments

	Filters' use	Switch off risky programmes	Secondary email account	Complicated passwords
More than 5 hrs	2.11129	2.29787	1.84452	2.29787
Between 1 and 5 hrs	1.84815	2.20364	1.64031	2.11686
Less than 1hr	1.55614	1.92950	1.18016	1.80418
No regular access	1.11475	1.66120	1.07650	1.46995
Average	1.81543	2.14735	1.58097	2.06792

Table 4. Behavioural Strategies –International Sample

	I am careful about which friend requests to accept	I only share things with close friends	I am careful which links or videos I click on to when I search for something	I avoid clicking on things that look weird or suspicious	I sometimes cover the webcam to prevent being seen	I am careful what pictures I share or post	I am careful what I say or post about myself	I limit talking online just to people I know	I limit online activities to apps or websites I trust
Very true	50%	51%	42%	55%	39%	50%	52%	45%	45%
A bit true/Some what true	41%	37%	47%	38%	30%	40%	40%	39%	44%
Not true	9%	12%	11%	7%	31%	10%	8%	16%	11%

Table 5. Children Being Careful When Talking and Posting About Themselves

Asia Pacific	All countries	Indonesia	Japan	South Korea	Australia	Taiwan
Very true	52%	63%	42%	31%	69%	54%
A bit true/Somewhat true	40%	33%	37%	56%	30%	44%
Not true	8%	0.04	20%	14%	1%	2%

Table 6. Reactive Strategies for Unwanted Disturbing Content

Asia Pacific	Total
Stop/get rid of it immediately by closing the page, deleting the file, or scrolling away	59%
Block the website	29%
Talk about it with your parent(s)/guardian(s)	26%
Use a program that prevents this from happening again	16%
Talk about it with a friend	15%
Look away or close your eyes	18%
Keep looking	12%
Talk about it with a brother/sister	8%

Table 7. Reactive Strategies for Unwanted Disturbing Content - Exposed Children

Asia Pacific	Total
Stop/get rid of it immediately by closing the page, deleting the file, or scrolling away	72%
Block the website	31%
Talk about it with your parent(s)/guardian(s)	18%
Use a program that prevents this from happening again	21%
Talk about it with a friend	23%
Look away or close your eyes	22%
Keep looking	15%
Talk about it with a brother/sister	9%

Table 8. Reactive Strategies for Unwanted Disturbing Content by Country

Asia Pacific	Indonesia	Japan	Korea	Australia	Taiwan
Stop/get rid of it immediately by closing the page, deleting the file, or scrolling away	60%	51%	53%	65%	64%
Block the website	31%	15%	28%	26%	28%
Talk about it with your parent(s)/guardian(s)	25%	16%	32%	45%	30%
Talk about it with a friend	19%	8%	17%	14%	19%
Use a program that prevents this from happening again	27%	5%	14%	13%	18%
Look away or close your eyes	32%	13%	9%	18%	20%
Keep looking	21%	8%	7%	7%	10%

Table 9. Reactive Strategies for Unwanted Disturbing Messages

Asia Pacific	All countries
Block and report the person	37%
Delete the contact	40%
Ignore the messages and the person	47%
Talk with parent(s)/guardian(s) about what to do	34%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	21%
Talk with brothers/sisters about what to do	10%
Talk with a teacher/lecturer about what to do	7%
Report the issue to the police and show them what happened	3%

Table 10. Reactive Strategies for Unwanted Disturbing Messages - Exposed Children

	All countries
Block and report the person	52%
Delete the contact	52%
Ignore the messages and the person	60%
Talk with parent(s)/guardian(s) about what to do	20%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	33%
Talk with brothers/sisters about what to do	11%
Talk with a teacher/lecturer about what to do	7%
Report the issue to the police and show them what happened	5%

Table 11. Reactive Strategies for Unwanted Disturbing Messages by Country

Asia Pacific	Indonesia	Japan	Korea	Australia	Taiwan
Delete the contact	47%	22%	35%	52%	46%
Block and report the person	45%	18%	36%	42%	47%
Ignore the messages and the person	52%	49%	43%	39%	49%
Talk with parent(s)/guardian(s) about what to do	33%	27%	30%	49%	33%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	36%	5%	16%	26%	24%
Talk with brothers/sisters about what to do	16%	4%	5%	13%	11%

Table 12. Reactive Strategies for Unwanted Disturbing Messages by Gender

Asia Pacific	Male	Female
Block and report the person	36%	39%
Delete the contact	37%	43%
Ignore the messages and the person	49%	45%
Talk with parent(s)/guardian(s) about what to do	36%	32%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	21%	21%
Talk with brothers/sisters about what to do	11%	9%

Table 13. Reactive Strategies for Unwanted Disturbing Messages by Age Group

	9-12	13-15	16-17	18
Block and report the person	31%	36%	37%	57%
Delete the contact	36%	39%	42%	51%
Ignore the messages and the person	35%	48%	55%	58%
Talk with parent(s)/guardian(s) about what to do	47%	36%	18%	11%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	16%	24%	19%	22%
Talk with brothers/sisters about what to do	10%	12%	9%	12%
Talk with a teacher about what to do	7%	7%	6%	5%
Report the issue to the police and show them what happened	2%	1%	4%	5%

Table 14. Reactive Strategies for Misuse of Personal Information

	All countries
Change the password	49%
Review privacy settings and choose a more secure password	34%
Use the report button	36%
De-tag yourself	26%
Ask your parent(s)/guardian(s) to help	28%
Disable or delete your account	23%
Report to the game's admin asking to ban the hacker and restore your account	16%
Ask to remove the photo or tag	12%
Tell the network about it in some other way and ask for another password/safer account	10%
Create a new profile and send new friend requests (perhaps telling them what happened)	11%
Use a support line or a hotline to report someone using a fake profile	8%
Provide false data	5%
Politely ask for the account back	5%

Table 15. Reactive Strategies For Misuse of Personal Information - Exposed Children

	All countries
Change the password	66%
Review privacy settings and choose a more secure password	55%
Use the report button	54%
De-tag yourself	45%
Ask your parent(s)/guardian(s) to help	15%
Disable or delete your account	29%
Report to the game's admin asking to ban the hacker and restore your account	31%
Ask to remove the photo or tag	28%
Tell the network about it in some other way and ask for another password/safer account	20%
Create a new profile and send new friend requests (perhaps telling them what happened)	18%
Provide false data	9%
Politely ask for the account back	14%
Asia Pacific	All countries

Table 16. Reactive Strategies for Misuse of Personal Information by Country

	Australia	Indonesia	Japan	South Korea	Taiwan
Change the password	51%	60%	34%	47%	55%
Review privacy settings and choose a more secure password	33%	44%	18%	39%	35%
Use the report button	44%	44%	15%	41%	36%
De-tag yourself	27%	29%	18%	23%	35%
Ask your parent(s)/guardian(s) to help	42%	17%	22%	28%	32%
Disable or delete your account	29%	21%	22%	20%	24%
Report to the game's admin asking to ban the hacker and restore your account	21%	12%	3%	15%	27%
Ask to remove the photo or tag	20%	15%	2%	6%	20%
Tell the network about it in some other way and ask for another password/safer account	13%	15%	1%	5%	15%
Create a new profile and send new friend requests (perhaps telling them what happened)	9%	16%	6%	10%	12%
Use a support line or a hotline to report someone using a fake profile	7%	10%	3%	9%	12%
Provide false data	3%	9%	1%	6%	6%
Politely ask for the account back	8%	8%	0%	4%	6%

Table 17. Reactive Strategies for Online Approaches and Meeting Requests

<i>What would you do if a stranger got in touch with you online?</i>	Asia Pacific	<i>What would you generally do if someone you met online asked you to meet him/her in person?</i>	Asia Pacific
Ignore him/her	51%	Refuse to meet	54%
Ask my parent(s), guardian(s) if they know this person	26%	Seek advice from your parent(s)/guardian(s)	31%
Ask my friends if they know this person	22%	Seek advice from your friends	13%
Reply to his/her request but only allow him/her to see a limited profile	20%	Agree to meet only if a friend would go with you	16%
Close the page or turn off the computer	18%	Agree to meet only if the stranger is more or less your age	10%
Reply to his/her request or messages	14%	Agree to meet only if a brother/sister would go with you	10%
Temporarily respond yes to his/her request and then delete it shortly after	12%	Agree to meet them	5%

Table 18. Reactive Strategies for Online Approaches and Meeting Requests

<i>What do you do when a stranger gets in touch with you online?</i>	Asia Pacific
Ignore him/her	47%
Ask my parent(s), guardian(s) if they know this person	15%
Ask my friends if they know this person	38%
Reply to his/her request but only allow him/her to see a limited profile	39%
Close the page or turn off the computer	10%
Reply to his/her request or messages	28%
Temporarily respond yes to his/her request and then delete it shortly after	19%

Table 19. Reactive Strategies for Online Approaches by Country

<i>What would you do if a stranger got in touch with you online?</i>	Australia	Indonesia	Japan	South Korea	Taiwan
Ignore him/her	59%	35%	46%	47%	69%
Ask my parent(s), guardian(s) if they know this person	40%	22%	14%	20%	31%
Ask my friends if they know this person	28%	31%	5%	23%	25%
Reply to his/her request but only allow him/her to see a limited profile	10%	47%	6%	22%	13%
Close the page or turn off the computer	17%	12%	12%	20%	29%
Reply to his/her request or messages	6%	36%	6%	12%	9%
Temporarily respond yes to his/her request and then delete it shortly after	7%	21%	3%	13%	16%

Table 20. Reactive Strategies for Meeting Requests by Country

<i>What would you generally do if someone you met online asked you to meet him/her in person?</i>	Australia	Indonesia	Japan	South Korea	Taiwan
Refuse to meet	73%	32%	53%	63%	53%
Seek advice from your parent(s)/guardian(s)	34%	34%	21%	29%	38%
Seek advice from your friends	10%	22%	8%	13%	13%
Agree to meet only if a friend would go with you	11%	26%	3%	14%	27%
Agree to meet only if the stranger is more or less your age	4%	28%	6%	6%	8%
Agree to meet only if a brother/sister would go with you	6%	18%	1%	10%	15%
Agree to meet them	0%	15%	3%	3%	4%

Table 21. Reactive Strategies for Cyber-Bullying

Asia Pacific	All countries
Block and report the person	45%
Delete the contact	43%
Talk with parent(s)/guardian(s) about what to do	38%
Show the person you are not bothered by their behaviour by ignoring them	27%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	19%
Talk with brothers/sisters about what to do	13%
Talk with a teacher about what to do	13%
Report the issue to the police and show them what happened	9%

Table 22. Reactive Strategies for Cyber-Bullying - Exposed Children

Asia Pacific	All countries
Block and report the person	54%
Delete the contact	63%
Talk with parent(s)/guardian(s) about what to do	29%
Show the person you are not bothered by their behaviour by ignoring them	39%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	38%
Talk with brothers/sisters about what to do	17%
Talk with a teacher about what to do	16%
Report the issue to the police and show them what happened	14%

Table 23. Reactive Strategies for Cyber-Bullying by Country

Asia Pacific	Australia	Indonesia	Japan	South Korea	Taiwan
Block and report the person	49%	56%	22%	45%	50%
Delete the contact	52%	51%	26%	37%	48%
Talk with parent(s)/guardian(s) about what to do	50%	22%	35%	37%	45%
Show the person you are not bothered by their behaviour by ignoring them	25%	24%	22%	26%	38%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	24%	32%	3%	16%	23%
Talk with brothers/sisters about what to do	12%	20%	5%	9%	16%
Talk with a teacher about what to do	16%	7%	8%	10%	22%
Report the issue to the police and show them what happened	11%	5%	6%	11%	14%

APPENDIX D: Age Group Variations in the Adoption of Resilience Strategies

Preventive Strategies

Technical Preventive Strategies

The data shows that younger children are less likely to adopt technical preventive strategies, in line with previous research and the literature comparing resilience with digital literacy. This result is particularly striking for the use of software protecting from unwanted content and for the use of secondary accounts. Surprisingly, the percentage of younger children using child friendly search engine is not higher than the one of their more senior fellows.

Table 3. Instrumental Actions International level Younger vs. Older Kids

9-12 years old	Use child friendly search engines	Have filters and software against unwanted content or contacts	Make my profile unavailable to the general public	Modify privacy settings to keep me away from unwanted contacts	Turn off programmes that I consider risky	Use a secondary account for spam	Use complicated, safe passwords	Keep my passwords completely secret from anyone
Very likely	25%	28%	26%	29%	35%	15%	29%	43%
Fairly likely	31%	28%	39%	31%	34%	28%	34%	37%
Not that likely	21%	19%	17%	17%	15%	22%	18%	10%
Not at all likely	7%	4%	6%	6%	4%	12%	6%	4%
Don't Know	16%	21%	11%	17%	12%	23%	13%	6%
18 years old								
Very likely	25%	30%	41%	45%	46%	27%	38%	62%
Fairly likely	41%	50%	44%	44%	41%	49%	48%	32%
Not that likely	24%	15%	13%	10%	12%	22%	12%	3%
Not at all likely	5%	1%	1%	1%	1%	3%	1%	1%
Don't Know	3%	4%		1%			1%	1%

Behavioural Preventive Strategies

According to age group no overwhelming variations are present, with the entire age sample (9-18) showing high levels of behavioural preventive strategies when online. Despite this, it is worth noting that 18 year olds across the board demonstrate slightly higher levels of behavioural preventive strategies, with the likelihood of 18 year olds being careful about what they say or post about themselves (63% very true) having the most significant variation when compared to 46% (very true) of 9-12 year olds. In addition, older teens are also more likely to be careful about which friends requests to accept (63% very true) when compared to 9-12 year olds (47% very true), as illustrated in table 6.

Table 6. Behavioural Preventive Strategies by Age Groups

9-12 years old	I am careful about which friend requests to accept	I only share things with close friends	I avoid clicking on things that look weird or suspicious	I am careful what pictures I share or post	I am careful what I say or post about myself	I limit talking online just to people I know	I limit online activities to apps or websites I trust
Very true	47%	51%	51%	44%	46%	45%	45%
A bit true/Somewhat true	43%	35%	40%	43%	41%	36%	41%
Not true	10%	14%	9%	13%	13%	19%	15%
NET: True	90%	86%	91%	87%	87%	81%	85%
18 years old							
Very true	63%	50%	61%	65%	63%	47%	46%
A bit true/Somewhat true	36%	44%	37%	32%	36%	39%	45%
Not true	1%	7%	3%	3%	1%	14%	9%
NET: True	99%	93%	97%	97%	99%	86%	91%

Reactive Strategies

Unwanted Disturbing Content

The age group analysis reveals several important differences across ages which, at the same time are not surprising. Older children aged from 16-18 tend to adapt more instrumental actions than communicative strategies compared to their younger fellows. As an illustration, while 61% of 18 year olds get immediately rid of the unwanted content, 53% of kids aged 9-12 do the same. On the contrary, children ask for parental advice (43%) way more than their older fellows (10%). Logically, younger children do not necessarily know how to react (7%) contrary to children who are 18 (1%).

Table 10. Reactive Strategies for Unwanted Disturbing Content by Age Group

	All countries
Block and report the person	52%
Delete the contact	52%
Ignore the messages and the person	60%
Talk with parent(s)/guardian(s) about what to do	20%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	33%
Talk with brothers/sisters about what to do	11%
Talk with a teacher/lecturer about what to do	7%
Report the issue to the police and show them what happened	5%

Disturbing Messages

Age Group

In line with the age distinctions made for responding to disturbing online content, younger children aged between 9 and 12 are less likely to adopt instrumental reactive strategies (deleting the contact) when compared to their older counterparts (36% vs. 51% for 18 year olds). Furthermore, older teens are more likely to ignore the messages (55% for 16 to 17 year olds and 58% for 18 year olds) and are much less likely to use communicative strategies (only 11% of 18 year olds would talk about it with their parents compared to 47% for 9 to 12 year olds).

Misuse of Personal Information

Although unsurprising, the age group distinctions illustrate some key variants in preventative strategies. Older teens are the most likely to adopt all forms of instrumental strategies, with 56% of 18 year olds changing their password and 42% de-tagging themselves. Moreover, 13-15 year olds are nearly twice as likely as 9-12 year olds to disable their account at 27%. Contrastingly, young children (9-12) are more likely to seek help from their parents or guardians (39%) when compared to their older counterparts (only 8% for 18 year olds). Once again, 10% of 9 to 12 year olds don't know how to react, against only 1% of 18 year olds.

Table 20. Reactive Strategies for the Misuse of Personal Information by Age Group

	9-12	13-15	16-17	18
Change the password	38%	54%	54%	56%
Review privacy settings and choose a more secure password	25%	34%	34%	36%
Use the report button	30%	35%	32%	37%
De-tag yourself	17%	29%	30%	42%
Ask your parent(s)/guardian(s) to help	39%	30%	14%	8%
Disable or delete your account	15%	27%	25%	20%
Report to the game's admin asking to ban the hacker and restore your account	13%	13%	16%	25%
Ask to remove the photo or tag	7%	11%	13%	22%
Tell the network about it in some other way and ask for another password/safer account	8%	8%	11%	14%
Create a new profile and send new friend requests (perhaps telling them what happened)	8%	11%	11%	12%
Use a support line or a hotline to report someone using a fake profile	4%	9%	12%	12%
Provide false data	4%	6%	6%	8%
Politely ask for the account back	4%	2%	5%	7%
Other, (please write what you would do)	0%	1%	0%	
Don't Know	10%	6%	8%	1%

Online Approaches and Meeting Requests

The age group analysis reiterates some of the main trends mentioned previously, with older teenagers (62% for 16-17 year olds and 66% for 18 year olds) being more inclined to adopt preventative strategies (ignoring the contact). Moreover, younger children (37% for 9-12 year olds) are much more likely to speak to their parents or guardians when implementing communicative strategies when compared to 18 year olds (10%) who opt to ask their friends if they know the person in question (24% for 16-17 year olds).

Table 25. Reactive Strategies for Online Approaches by Age Group

<i>What would you do if a stranger got in touch with you online</i>	9-12	13-15	16-17	18
Ignore him/her	44%	56%	62%	66%
Ask my friends if they know this person	18%	25%	20%	24%
Ask my parent(s), guardian(s) if they know this person	37%	25%	12%	10%
Reply to his/her request but only allow him/her to see a limited profile	17%	17%	18%	16%
Close the page or turn off the computer	19%	18%	21%	31%
Reply to his/her request or messages	8%	17%	10%	11%
Temporarily respond yes to his/her request and then delete it shortly after	11%	11%	13%	21%
Other, (please write what you would do)	1%		0%	
Don't Know	9%	6%	6%	1%

When responding to an invitation from an unknown contact to meet offline communicative strategies again highlight significant age differences, with 9-12 year olds (41%) more than twice as likely as 18 year olds (18%) to seek advice from a parent or guardian. Significantly, a smaller percentage of the 9-12 and 18 age groups (48% for both) stated they would refuse to meet the contact (59% for 13-15 and 58% for 16-17). However, only 3% of 9-12 year olds stated they would agree to meet, compared to 12% for 18 year olds.

Table 26. Reactive Strategies for Meeting Requests by Age Group

What would you generally do if someone you met online asked you to meet him/her in person?	9-12	13-15	16-17	18
Refuse to meet	48%	59%	58%	48%
Seek advice from your parent(s)/guardian(s)	41%	33%	20%	18%
Seek advice from your friends	11%	13%	15%	17%
Agree to meet only if a friend would go with you	12%	17%	21%	37%
Agree to meet only if the stranger is more or less your age	12%	7%	10%	14%
Agree to meet only if a brother/sister would go with you	9%	14%	11%	10%
Agree to meet them	3%	7%	5%	12%
Other, (please write what you would do)	2%	0%	0%	1%
Don't know	7%	4%	5%	1%

Cyber Bullying

The age group analysis further supports the previous distinctions made, with older teenagers from 16-18 choosing to adopt a more instrumental approach to cyber bullying by deleting the contact (54% of 18 year olds). Moreover, younger children are much more likely to use communicative strategies (51% for 9-12 year olds) when compared to only 24% for 18 year olds. The older respondents were also much more likely to use disengagement strategies by ignoring the person (42%) when compared to their younger counterparts (19% for 9-12 year old children).

Table 30. Reactive Strategies for Cyber-Bullying by Age Group

	9-12	13-15	16-17	18
Delete the contact	35%	44%	47%	54%
Block and report the person	39%	42%	44%	54%
Talk with parent(s)/guardian(s) about what to do	51%	38%	26%	24%
Show the person you are not bothered by their behaviour by ignoring them	19%	28%	31%	42%
Ask the person to stop sending annoying messages or to delete an embarrassing picture	15%	21%	19%	20%
Talk with brothers/sisters about what to do	11%	17%	11%	19%
Talk with a teacher about what to do	16%	12%	9%	13%
Report the issue to the police and show them what happened	7%	9%	10%	16%
Other, (please write what you would do)	2%	0%	0%	
Don't Know	6%	5%	5%	1%