A Survey and Analysis of the China’s Child Cybersecurity

Professor. LU Chuanying
Internet Development Research Institution of Peking University
Shanghai Association for Artificial Intelligence and Social Development
Shanghai Institutes for International Studies
Sampling

Targeting children aged 8-12, a questionnaire survey is done both online and offline in 15 provinces and cities across China.

**The quota distribution is as follows:**

- **Regions:** East China 2,933 (47.0%), Central China 1189 (19.1%), Southwest 795 (12.7%), Northwest 786 (12.6%), North China 536 (8.6%).
- **Urban/rural division:** Provincial capital city/municipalities 5,727 (91.8%), prefecture-level cities 255 (4.1%), county-level cities/towns 148 (2.4%), and rural 99 (1.6%).
- **Gender:** Male 3,068 (49.2%), and female 3,171 (50.8%).
- **Identity:** Children 6,012, parents 905, and teachers 323.
- **Relationships:** Couples 351, mothers 520, and grandparents 34.

**In-depth interview:**

- This project team has identified focus groups and key issues, selecting 26 children and 9 parents by snowball sampling.
Children's digital life enriched

According to this study, 87.1% of children have already started their digital life, in which 73.8% own Internet access devices. Children's key Internet access terminals are tablet computers, smartphones, and smartwatches. Regarding the convenience of Internet access, approximately 30% of children can surf the Internet freely at home, while 16.5% can surf the Internet freely in school. (50% of children are online with their parents, indicating that supervision is in place. But how to supervise?)

Children's online activities mainly include schooling, socializing, and entertainment. After the COVID-19 outbreak, online schooling has become an inevitable choice. The penetration rates of online schooling and chatting among children are as high as 84% and 70%, and more than 40% of children engage in online entertainment activities such as live webcasts, videos, music, and games. 13% of children publish pictures, texts, audio, or video works on the Internet, and nearly 10% of children participate in online forums. (What is the purpose of participating in the forum? Need in-depth research in game forums)

The diversity and participation of boys in online activities are generally higher than girls while girls are slightly more involved in learning than boys, while the proportion of boys participating in online games is 20% higher than girls.
Child cybersecurity facing challenges

① As this study finds out, more than 90% of children have been digitally harmed at least once or experienced digital hazards, with their psychological, physical, social, and financial well-being and their privacy and other digital rights threatened. The risk of digital rights being violated is the highest, followed by psychological and social risks, while obvious risks such as financial and physical risks are rather low, which shows that the risks in children’s digital environment are hidden or latent. **High risk of content and engagement, low risk of exposure.**

② **Levels and types of child cybersecurity risks based on their incidence:**

**level 1:** Inappropriate self-disclosure, ad push, Internet addiction, dangerous imitation, undesirable content, social grooming, and community grooming is very high (over 60%) for children. These risks deserve more attention also because they are hidden and the negative impacts are difficult to detect in a short time.

**level 2:** The incidence of more serious child cybersecurity risks such as cyber deception and cyberbullying is over 40%.

**level 3:** The incidence of excessively tipping online streamers and account leaks among children is around 30%.

**level 4:** The incidence of hidden cybersecurity threats such as Internet indecency facing children is as high as 12%.

Is there a problem with this data? The incidence is used, not the frequency. Using the mean for the degree of use, 88% chose "never", but what about "occasionally"? What kind of children (boys/girls) would expose their private parts under what circumstances? How to define private parts?
Children are both recipients, participants, and perpetrators of online content or digital activities, where the risks they face as recipients of content and perpetrators of behavior are higher than the exposure risks they face as participants.

40% of children are often exposed to undesirable information on the Internet, and there are hidden dangers of evil in videos and live broadcasts.

80% of children have experienced online friendships, 14.2% of children believe that almost every one of their classmates has an online friend, and 30% of children have half of their classmates have online friends.

“Ultraman and princess fairy tale cartoons and live-action funny videos are the favored videos for children, but occasionally they encounter sudden horror, gore, violence, indecency, and other content.”

Figure 5. Comparison of three dimensions of risks
Children’s cybersecurity risk awareness goes before their risk prevention competence

① Children in China are more vigilant about cybersecurity risks like leakage of personal information and Internet addiction. They are cautious about socializing with strangers but have a low awareness of cybersecurity risks arising from content, ad push, or temptation by online friends or acquaintances.

② It must be noted that children’s skills and capabilities to fend off cybersecurity risks are even weaker. First, children are less vigilant against perceived risks if they are offered any material benefit or emotional temptation. Second, they lack the necessary digital literacy and skills to respond to risks of cyber violence, device and account safety, and ad push.

③ Daily instructions by parents at home and teachers in school (including safety literacy classes) and mass media reports are the key ways for children to acquire cybersecurity knowledge. More than 70% of parents and over 60% of teachers will warn children against cybersecurity risks.
Parents vary in cybersecurity awareness and generally lack digital parenting skills

① When it comes to cybersecurity for their children, parents generally believe that the most common parenting method should be protective and instructive. In fact, according to the survey, controlling, forbidding, and restrictive methods are their most commonly used digital parenting methods. Of the 12.9% of children who have never gone online, more than 71% are prevented from accessing the Internet by their teachers or parents. Of the 73.8% of children who have their own digital devices, only 40% can surf the Internet freely. In addition, only about 2% of parents do not limit screen time for their children.

② Only 32.9% of child respondents believe that their parents activate the "kids’ mode" often. In-depth interviews with children find that the "kids’ mode" could prevent children from getting addicted to the Internet if parents take it seriously.

table1. Principal factors of digital parenting

<table>
<thead>
<tr>
<th>Parenting Method</th>
<th>Item</th>
<th>Factor Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protective Parenting</td>
<td>I tell children what messages can’t be posted online</td>
<td>4.0978</td>
</tr>
<tr>
<td></td>
<td>I prevent my children to put personal information on the Internet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When children access the Internet, I activate the “kids’ mode”</td>
<td></td>
</tr>
<tr>
<td>Instructive Parenting</td>
<td>I teach children how to tell the difference between true and false information online</td>
<td>4.0290</td>
</tr>
<tr>
<td></td>
<td>I often try to answer my children’s questions about digital activities.</td>
<td></td>
</tr>
<tr>
<td>Restrictive Parenting</td>
<td>I will limit my child's time on the Internet</td>
<td>4.0189</td>
</tr>
<tr>
<td></td>
<td>I have taught my children how to recognize online ads or sales pitches</td>
<td></td>
</tr>
<tr>
<td></td>
<td>I impose restrictions on downloading content from the Internet</td>
<td></td>
</tr>
<tr>
<td>Forbidding Parenting</td>
<td>I will decide what my children do or do not do online</td>
<td>3.9483</td>
</tr>
<tr>
<td></td>
<td>I give examples to raise children’s awareness of the consequences of overusing the Internet.</td>
<td></td>
</tr>
</tbody>
</table>
Teachers have the highest awareness of and concerns over child cybersecurity risks, but have got little support.

- Teachers report the highest level of concern and awareness, much higher than parents. But teachers' awareness of risks of hidden but more serious harm, such as cyber clairvoyance and divination, pornography, and inappropriate videos, falls behind parents.
- Teachers are aware of the importance of ICT literacy, hold a positive attitude towards children's Internet access, and attach importance to ICT literacy education and supervision, but they are relatively weak in helping students solve problems or providing practical support.
- Educational background has a significant effect on improving teachers' digital training ability. The higher degree a teacher obtains, the stronger his or her ability is in giving digital literacy instructions to children.
- Teachers play an exemplary role in children's digital skills development. Their use of digital devices in front of children and their comments on digital living is important for raising children's awareness of cybersecurity risks.
Proper digital parenting can reduce children’s cyber vulnerability.

Cybersecurity awareness education, control over Internet use, and network support in the family show significant negative correlations with child cybersecurity risks, which means all three factors of family digital education can help control children’s cybersecurity risks. Among them, family control over Internet use and digital literacy education can reduce child cybersecurity risks most significantly and can be considered as the most effective forms of digital parenting.

Figure 19 Correlation between digital parenting and child cybersecurity risks
ICT education in school is an important means of controlling child cybersecurity risks.

As the figure shows, ICT literacy education, ICT support, and teachers' attitudes towards ICT are all negative correlation with child cybersecurity risks, which means they can help control cybersecurity risks.

![Figure 20 Correlation between ICT education in school and child cybersecurity risks](image-url)
01 Child cybersecurity Policy Recommendations

① **Government: Building mechanisms to promote child cybersecurity.**
   1. Enacting laws and regulations build a child cybersecurity shield.
   2. Taking policy-based actions to create a sound social system.
   3. Fostering a healthy well-regulated digital market for children.
   4. Bridging the gap between Internet use and digital literacy.

② **Business: Creating a children-friendly digital environment**
   3. Developing innovative technologies and methods to ensure child cybersecurity.
③ Social organizations and specialized institutions: Raising awareness of child cybersecurity risks and enhancing risk-mitigating capabilities

1. Cultivate specialized talent and form a child cybersecurity research and education network.
2. Popularizing knowledge of digital child safety and raising parents’ and teachers' risk awareness and education competence.
3. Building industry and professional exchange platforms to improve child cybersecurity management.

figure 21. BEANO: Digital platform for children

figure 22. KFC restaurant holds children's cyber safety science activities
④ **Family: Attaching importance to self-education and taking care of children's digital life**
1. Strengthening self-education, raising cybersecurity awareness, and improving their competence in digital education
2. Increasing parent-child interaction and working as a guide, mentor, and companion for children in the digital world
3. Resorting to "emotional warmth" rather than "cold rejection", and cultivating children's judgment and resilience in cyberspace

⑤ **Prioritizing and institutionalizing cybersecurity education**
1. Developing a cybersecurity education curriculum based on age level and incorporating it into the school performance evaluation system
2. Strengthening specialized training for teachers to raise their awareness of digital child safety risks and their ability to cope with key issues
3. Building labs or practice bases for children to gain cybersecurity experience.
Tip 1: Principal factors of cybersecurity parenting

◆ I tell children what messages can't be posted online
◆ When children access the Internet, I activate the "kids’ mode"
◆ I teach children how to tell the difference between true and false information online
◆ I impose restrictions on downloading content from the Internet
◆ I give examples to raise children’s awareness of the consequences of overusing the Internet.
◆ I ask child not to chat with strangers online
I tell students not to disclose or share personal information on the Internet.

When students access the Internet, I activate the "kids’ mode".

The school offers courses to teach students how to surf the Internet safely.

I teach students to identify the authenticity of information on the Internet.

I give examples to raise students’ awareness of the consequences of overusing the Internet.

I ask students not to chat with strangers online.

I always remind students to ask adults for help when they encounter difficulties online.

I have received systematic training in instructing students to be safe online.

I take the initiative to learn about training related to student safety online.