Safeguarding Children in Digital Spaces

For Prelims: Metaverse, Virtual Reality, Artificial Intelligence, child online safety toolkit, Safety by design

For Mains: Impact of cyberbullying and online sexual exploitation on children, Issues Related to Children

Source: TH

Why in News?

Recently, heightened concerns have emerged regarding c**hildren's safety in digital spaces.** Rising incidents of **online exploitation** have prompted calls for urgent action. Amid evolving digital landscapes, safeguarding children's rights is paramount.

What are the Challenges for Children in the Digital Spaces?

- **Cyberbullying:**
  - **Definition:**
    - **Cyberbullying** is the use of digital platforms to harass, threaten, humiliate, or harm another person, especially a peer.
  - **Forms:**
    - Abusive messages, rumours, hurtful comments, sharing private or embarrassing photos or videos, impersonating someone, or excluding someone from online groups.
  - **Impact:**
    - Negative effects on children's mental health, self-esteem, academic performance, and social relationships. It can also lead to anxiety, depression, isolation, self-harm, or suicide.
- **Online Sexual Exploitation and Abuse:**
  - **Definition:**
    - It is the use of digital platforms to **engage children in sexual activities or expose them to sexual content**, for the gratification or profit of the offender.
  - **Forms:**
    - Producing, distributing, or accessing child sexual abuse material, grooming children for sexual purposes, soliciting children for sexual acts, livestreaming sexual abuse, or **sextortion.**
  - **Effects:**
    - Can have devastating effects on **children's physical, psychological, and emotional health,** and can cause lifelong trauma and damage.
- **Privacy and data protection:**
  - **Definition:**
    - Privacy and data protection is the right of children to control their personal information and how it is collected, used, shared, or stored by others, especially online.
  - **Violations:**

        - It can be violated by tech companies, advertisers, hackers, or other third parties, who may collect, use, or sell children's data without their consent or knowledge, for commercial or malicious purposes.
    - **Consequences:**
        - Can have harmful consequences for children, such as **identity theft, fraud, targeted marketing, manipulation, discrimination**, or exposure to inappropriate or dangerous content or contacts.
- **Digital literacy and citizenship:**
    - **Definition:**
        - Digital literacy and citizenship is the ability and responsibility of children to use digital platforms effectively, safely, and ethically, and to participate in the online world as informed and active citizens.
    - **Challenges:**
        - It can be challenged by the **proliferation of misinformation, disinformation, and hate speech** online, which can mislead, confuse, or harm children, and undermine their trust and values.
    - **Consequences:**
        - Digital literacy can be hindered by the **lack of access, affordability, or quality of digital platforms** and technologies, which can create digital divides and inequalities among children.
- **Metaverse and Virtual Reality (VR):**
    - **Definition:**
        - The metaverse is a virtual world that uses virtual reality, augmented reality, and other advanced technology to allow people to have lifelike experiences online.
    - **Forms:**
        - Exploitation by virtual predators and **economic exploitation** through scams. **Harassment and discrimination** thrive in virtual environments, fostering cyberbullying and online discrimination based on users' identities.
        - Privacy violations are rampant, with **data mining and surveillance compromising** users' personal information and security.
    - **Negative Impacts of the Metaverse:**
        - Children may encounter graphic or violent content in virtual environments, leading to desensitization or emotional distress.
            - Continuous exposure to such content can desensitize children to violence or other inappropriate behaviours, impacting their emotional well-being.
- **Generative Artificial Intelligence (AI):**
    - **Definition:**
        - Generative AI refers to AI systems capable of producing new content, such as text, images, or music, based on patterns learned from existing data.
    - **Forms:**
        - Generative AI offers educational benefits and creative opportunities for children, but it also poses risks, including the **creation of persuasive disinformation and indistinguishable fake images, videos and information.**
    - **Vulnerabilities:**
        - Children's cognitive vulnerabilities make them susceptible to **misinformation, raising concerns** about the impact of AI-generated content on young minds.

Alarming Statistics on Online Child Safety

- **More than a third of young people** in 30 countries report being cyberbullied, with 1 in 5 skipping school because of it.
- 80% of children in 25 countries report feeling in danger of **sexual abuse or exploitation online.**
- **54% of those who regularly used the internet** as a child (now aged 18-20) were the victims of at least one online sexual harm, according to the WeProtect Global Alliance.

What Can Be Done to Keep Children Safe Online?

- **Prevention:**
  - Cyberbullying can be prevented and addressed by **educating children about online etiquette and empathy**, encouraging them to report any incidents, supporting the victims, and holding the perpetrators accountable.
  - Teaching children **about responsible VR usage, digital citizenship, and online safety.**
  - Digital literacy and citizenship can be enhanced by **teaching children how to access, evaluate, create, and share online content,** how to communicate and collaborate online, and how to respect and protect themselves and others online.
- **Tech Companies' Role:**
  - Tech firms must prioritize **'safety by design(SBD)',** acknowledging their role in safeguarding children's well-being online, as highlighted in recent Congressional hearings.
    - SBD puts user **safety and rights at the centre** of the design and development of online products and services. It focuses on the ways technology companies can **minimise online threats by anticipating, detecting and eliminating online harms** before they occur.
  - UNICEF recommends that tech companies apply the **highest existing data protection standards** to children's data in the **metaverse and virtual environments.**
- **Government Responsibilities:**
  - Assess and adjust **regulatory frameworks like the** Child Abuse Prevention and Investigation Unit **regularly to prevent violations** of children's rights in digital spaces.
  - Develop innovative initiatives like a **child online safety toolkit,** to help parents, educators, and other concerned adults protect children from online dangers.
  - Utilize regulatory power to combat harmful content and behaviour affecting children online.
- **Collective Responsibility:**
  - Recognize that **existing real-world rules for child protection** should extend to the online realm.
  - Emphasize the importance of collaboration between tech companies, governments, and organizations to ensure child safety online.

What are India's Initiatives Related to Cyber Security?

- **National Cyber Security Policy.**
- **Cyber Surakshit Bharat Initiative.**
- **Indian Cyber Crime Coordination Centre (I4C).**
- **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre).**
- **Computer Emergency Response Team - India (CERT-In).**
- **Critical information infrastructure (CII).**

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q.1 In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only

(c) 2 and 3 only
(d) 1, 2, 3 and 4

Ans: (b)

Q.2 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**