

Cybercrime Challenges in the ASEAN Region: Indonesian Situation on Cybercrime Against Children



DR. RARA ENDAH SULISTYANINGSIH, MSI
MINISTRY OF SOCIAL AFFAIRS OF THE REPUBLIC OF INDONESIA

The 2nd ASEAN Conference on Crime Prevention and Criminal Justice
Bangkok, 27-28 February 2020

Advantages of the Internet

- Entertainment
 - Online Streaming
- Education
 - E-mail, E-book, Online tutorials
- Transportation
 - Online Transportation, Taxi Services, Food Delivery
- Business & Entrepreneurship
 - online shop, online trading,
- **Communication:** Video Chatting, Messaging, Livestreaming
- **Health:** Applications for Health Information
- **Information:** Safe, fast access, and various of information for children



Disadvantages of the Internet



- **CYBERBULLYING:** attacks on social media by inappropriate words and expressions
- **CYBERCRIME:**
 - Invasion of Privacy
 - Sexual Exploitation
 - Human Trafficking
 - Pornographic Content
 - Online Predators
- **ADDICTIONS:**
 - On gadgets, social media, online games, pornography
- **HOAX:**
 - Fake News
 - Fake Identities
 - Incomplete Information



What is Cyber/Online Crime??

“an unlawful acts committed by using the computer as a tool or as a target or as both. This can involve criminal activities that are traditional in nature, such as theft, fraud, forgery (copy), defamation and mischief

Children and adolescents using the internet and associated technologies are often poorly equipped to fully understand the potential risk of being exposed to illegal activities committed through the use of ICTs.

Furthermore, violence against children committed through the use of ICTs is more difficult to detect and address than traditional forms of violence against children.

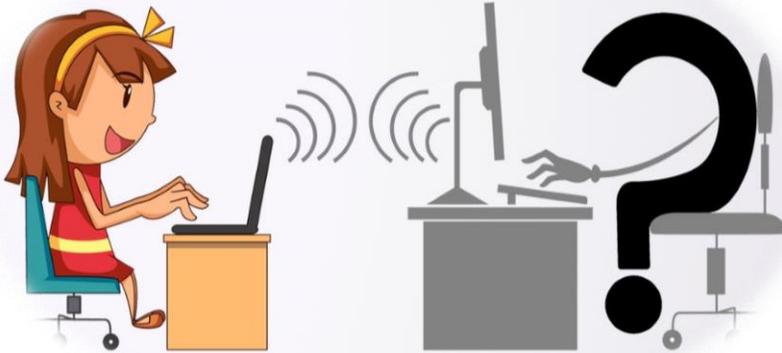


Cyber Crime against Children

Children and adolescents using the internet and associated technologies are more vulnerable to online abuse and exploitation than adults.



In 2018, Indonesia had more than 200 million cyber-attacks.



Percentage;
Per January 2019, 150 million people are using the internet
Thus represents 13% growth from the previous year.
For illustration → In only this February, Indonesia experienced 1.35 million web attacks

Cyber Crime is No Less Dangerous than any other Crime

Cybercrime and cybersecurity are issues that can hardly be separated in an interconnected environment. The fact that the UN General Assembly resolution on cybersecurity addresses cybercrime as one major challenge



This leads to cybercrime against children:

1. Child pornography
2. Child sexual exploitation
3. Child trafficking
4. Cyber bullying
5. Hate speech



Affecting:

- Child mental health
- Child social behaviour
- Physical well-being
- Child development

Downside:

- ✓ Stress and depression
- ✓ Mental disorder
- ✓ Suicidal attempt and suicidal thought
- ✓ Death rates
- ✓ Creating child social problem

What needs to be Done?

A holistic approach to fight cybercrime against children;

- Strengthening the law
- Adopting policies and regulation; legislative responses for child online protection
- Adoption of appropriate domestic law for child online protection
- Raising awareness
- Building capacity; establishing good coordination between institutions
- Proving technical assistance; developing secure digital infrastructure
- Developing the industry; develop the local cybersecurity industry



Must involve various stakeholders, including;

- Children
- Families
- Communities
- Governments
- Members of civil society
- Private sector

Legal Basis

- Law No. 35 of 2014 Amending Law on Child Protection No. 23 of 2002
- Law No. 10 of 2012 regarding the Legalisation of Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC)

Children's rights are part of human rights as contained in Article 28 B Clause (2) Second Amendment of 1945 Foundational Law (UUD 1945) in which "every child deserves to live, grow, and develop, protected from violence and discrimination."

The implementation of child protection in Indonesia should be based on Pancasila and UUD 1945 as well as United Nations Children's Rights Convention comprising foundational principles such as children's non-discrimination, best interest, right to live, right to grow and develop, and right to opinion being heard and valued

***Then we articulate the clause, the protection for the child should include child being protected from cyber crime, abuse, exploitation and violence**



Legal Basis



The Law No. 44 of 2008 concerning pornography (also known as “Law No. 44 of 2008 on pornography”) (hereafter also referred to as “Anti-Pornography Law”) criminalizes activities involving pornography, including pornography that explicitly contains child pornography.

The Act No. 13 concerning Manpower (hereafter referred to as “Manpower Act”) makes it an offense to make use of, procure, or offer children for prostitution, the production of pornography, or pornographic performance with a penalty of two to five years imprisonment, or a fine of 200 million to 500 million rupiah, or both. In addition, the Criminal Code punishes any person who engages in activities related to a writing of which the person knows the content, or a portrait or object known to the person to be offensive against decency.





Urgency

Child online abuse and exploitation is in urgent in Indonesia, as the increase level of number in child online sexual exploitation, the motive that being used is job offer with high paid salary

Increase number in child cases of pornography and cybercrime, as followed (source: KPAI) :

- 2014, 322 cases
- 2015, 463 cases
- 2016, 587 cases
- 2017, 608 cases
- 2018, 679 cases
- 2019, 653 cases (per July 2019)
this number is increasing by the end of 2019



Online child sexual exploitation cases:
Up to 40 children
Happened in between
January up to
February 2020

Action Plans

- Increasing society awareness to digital literacy, especially for parents and children
 - Creating positive movement or campaign on child protection
 - Assessing, evaluating and increasing the roles, functions of MoSA
 - Building up and strengthening the coordination in all level of government institutions and other stakeholders
- of Child Protection Law, Law No. 35 of 2014 in Child Protection
- Building a comprehensive national child protection system to prevent and respond to cyber violence, abuse, neglect and exploitation
 - Arranging and Drafting a Child Protection Act against Cyber Crime





Action Plans



- Support local governments in establishing integral child protection services at district/cities
- Socialization in every school in regards of cyber crime against children through programs that has been customizes by all level of governments (Directorate Social Rehabilitation for Children (MoSA), KPPPA, KPAI, etc.)
- Cooperation between MoSA and Indonesian National Police Department to detect the mafia of cyber crime against children

How do we stop cyber violence without giving up access to the Internet?

- Turn on a setting that uses artificial intelligence technology to automatically filter and hide content/post intended to harass or exploit people
- Encourage positive behavior and interactions by giving people tools to customize their experience on social media

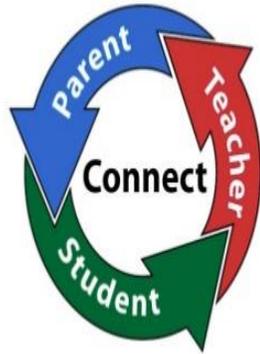


Action Plans

Teacher's Role To Prevent Cyber Crime

Continued.....

- Don't suffer in silence. If they are being bullied then they should tell their parents. If they don't feel to talk to them then tell a teacher or an adult that you trust. You mustn't keep it to yourself because if you do, the bully has got exactly what they want.
- They should be made aware about cyber bullying and that it is a punishable offence as per cyber law.



What school and parents can do to prevent cyber crime against children?

- Encourage both parents and children to be more thoughtful about what they share
- Encourage children to decide who can see their profile, send them direct messages or comment by adjusting their account privacy settings
- Report hurtful, harmful comments, messages and photos and request they be removed

What the Internet Companies should do?

- Introducing ways to address cyber crime and protect their users with new tools, guidance and ways to report online abuse
- Provide educational tools and guidance for children, parents and teachers to learn about risks and ways to stay safe online



Case Study : Child Trafficking at Social Rehabilitation Center Jakarta

- a. On 13th January 2020, Police had raid the Kafe Khayangan and arrested 10 child victim, 11 adult women, and 6 café's employees. The raid had been done because the police department got report from a child victim that has escaping successfully from Kafe Khayangan.
- b. After doing the case assessment by the police, on the 15th January 2020 as many as 8 children got referred to e Center to get further social rehabilitation and protection.
- c. The average age of the children that being in the shelter and in the process of rehabilitation is 15 – 18 years old.
- d. All the children victim Anak had recruited by some individuals who work in the café through online social media such as Facebook, they got offered to become shopkeeper and café waitress.
- e. All the children worked unknowingly by the parents that the children had to serve 'the guests'.
- f. Normally, the family of the child victim are in the lower economic status.

1. The Intervention :
 - Safe shelter protection,
 - Health screening,
 - Psychology screening,
 - Biopsychosocial assessment,
 - Physical therapy; children being given the understanding about their physical condition and encourage to do special treatment,
 - Psychosocial therapy; including the nourishment therapy, reality therapy, cognitive therapy, CBT,
 - Mental-spiritual therapy; including MFD (mental, physical, discipline), religious knowledge and education, read and write the Holy Book,
 - Family support, including parenting skill, family counselling, and reunification. Family support is presenting the family to get to know the child condition,
 - Livelihood therapy, including;
 - 1) *life skill*,
 - 2) *handy craft skills*

www.TheSteelMethod.com

STOP! CYBER CREEPS

Every year thousands of boys and girls become victims of cyber criminals. Remember these helpful tips to keep safe.

DON'T BE FOOLED



! Cyber creeps pretend to be someone else to gain trust and get your private information.

REMEMBER

NEVER GIVE AWAY:

- ⊗ Your NAME
- ⊗ Your PHONE NUMBER
- ⊗ Your ADDRESS
- ⊗ Your PASSWORD
- ⊗ Your SCHOOL NAME
- ⊗ Your PARENT'S NAME



! Cyber creeps can use this info to find you.

BE SMART

NEVER:

- ⊗ Agree to meet face-to-face
- ⊗ Send pictures of yourself
- ⊗ Respond to troubling E-mail



! **ALWAYS** let an adult you trust know if you get a **threatening** or **weird** E-mail.

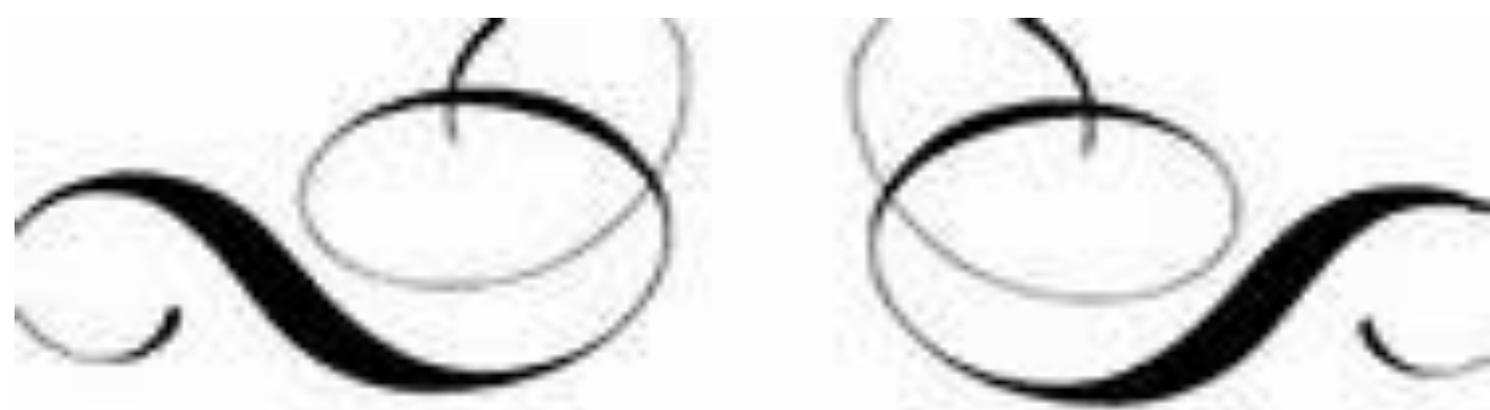
ATTENTION PARENTS:

- ✓ Talk to Your Kids
- ✓ Connect with Your Kids Online
- ✓ Observe, Don't Intrude
- ✓ Be Proactive



www.TheSteelMethod.com Brought to you by David Steel, social media strategist. To learn how David can help your organization leverage its online presence, call toll-free at: 1-888-832-7113

Act NOW
Before it's
TOO LATE!!!



Thank You

