Understanding Cybercrime Categories and Recent Developments in Cyberpornography

11 September 2024

Created by: Amiah Armstrong, Jasmyn Wilhelm, and Louis Ferrara

Table of Contents

Introduction

We will explore the realm of cybercrime in the following presentation, beginning with an explanation of its four primary classifications: cyberviolence, cybertrespass, cyberpornography, and cyber fraud.

We'll start by carefully explaining each category's definition and giving a comprehensive understanding of its properties and effects. Then, to emphasize the similarities and differences between these categories, we will compare and contrast them. Next, we'll examine a recent news article about the emerging area of cyberpornography.

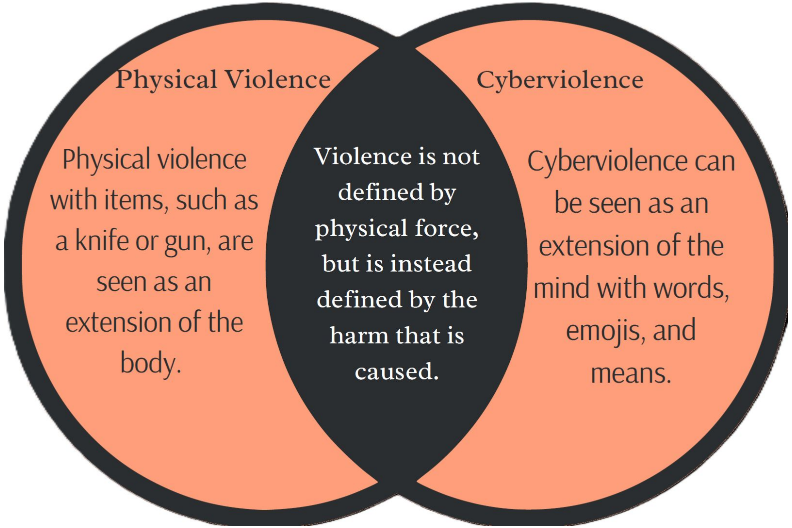
Together, we will explore the complicated nature of cybercrime and learn how these many categories influence our online environment.

Defining the Four Categories of Cybercrime

Cyberviolence

Definition: Activities that result in long-lasting psychological damage are categorized as cyberviolence.

Topics such as cyberfraud and cyberpornography receive more attention, but cyberviolence can do immense harm.



Physical Violence

Physical violence with items, such as a knife or gun, are seen as an extension of the body.

Violence is not defined by physical force, but is instead defined by the harm that is caused.

Cyberviolence

Cyberviolence can be seen as an extension of the mind with words, emojis, and means.

Types of cyberviolence

- Cyberbullying
- Cyberstalking
- Flaming
- Trolling
- CSAI / CSAM
- Internet-Facilitated Sex Trafficing
- Online Shaming
- Trolling
- Hate Speech
- Cyber Terrorism
- Cyber War

Cybertrespass

Definition: Unapproved entry into areas where titles and ownership rights have already been established within computer systems.

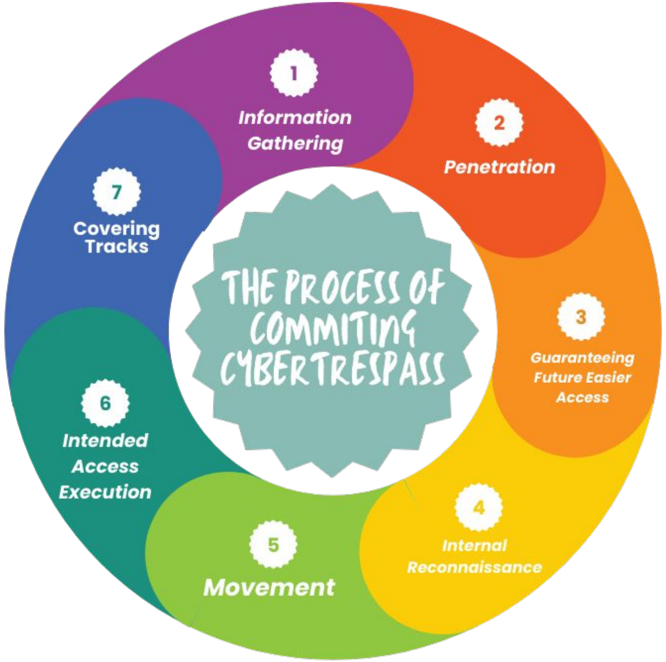
- ➔ Methods of Detection:
  - ◆ AI
  - ◆ Machine Learning
- ➔ Two explanations found throughout research:
  - ◆ Self-Control Theory
  - ◆ Social Bonding Theory

How offenders gain access:

- ➔ Impersonation
- ➔ Interception
- ➔ Malware
  - ◆ Viruses
  - ◆ Worms
  - ◆ Trojans
  - ◆ Ransomware

Types of Cybertrespass crimes:

- ➔ Data Theft
- ➔ Data Manipulation
- ➔ Altering Computer Operations

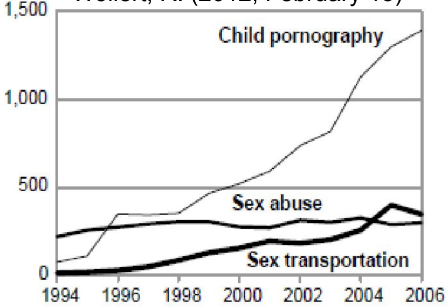

THE PROCESS OF COMMITING CYBERTRESPASS
1
Information Gathering
2
Penetration
3
Guaranteeing Future Easier Access
4
Internal Reconnaissance
5
Movement
6
Intended Access Execution
7
Covering Tracks

Cyberpornography

Defined by Wall: ***“the publication or trading of sexually expressive materials in the digital environment”.***

- ➔ Compared to before, there is more monetization on pornography, with producers charging customers to join sites or view specific content.
- ➔ Most forms of pornography are legal, especially in countries with free speech protections.
- ➔ What makes it a crime is when it involves extreme sexual acts, animals, and the exploitation of children.

Wollert, R. (2012, February 15)



Sexual deviance, pornography consumption, and sex work can be called ***victimless crimes****.*

But are they?

THE MILLER TEST
Is the material sexually explicit by the standards of the community?
Does the material show an explicit act of sex?
Is the material sexually explicit by the standards of the community?
Does the material have any societal value other than for sexual consumption?

Cyber Fraud

Definition: ***The act of lying and stealing in the digital environment.***

This encompasses both **CYBERDECEPTION** and **CYBERTHEFT.**

Identity Theft

Wrongfully Obtaining another person's personal information

Selling of Counterfeit Goods

Selling fake products that are marketed as legit

Romance Scams

Scammer pretends to form an emotional bond with victim in order to exploit them financially

Advance Fee Frauds

Scammer makes victim believe they will get paid for performing a specific action

Phishing

Fraudulent and unsolicited communication efforts

➔ Cyberfraud is a crime that can be experienced by anybody, no matter their age or class.

➔ Categorizing between money motivation and information motivation helps to organize new schemes.

➔ As technology becomes more advanced, more and more scams take form.

Fake emails

Psychic scams

Share scale

Loan scams

Person in distress fraud

419 scams

Bogus lottery

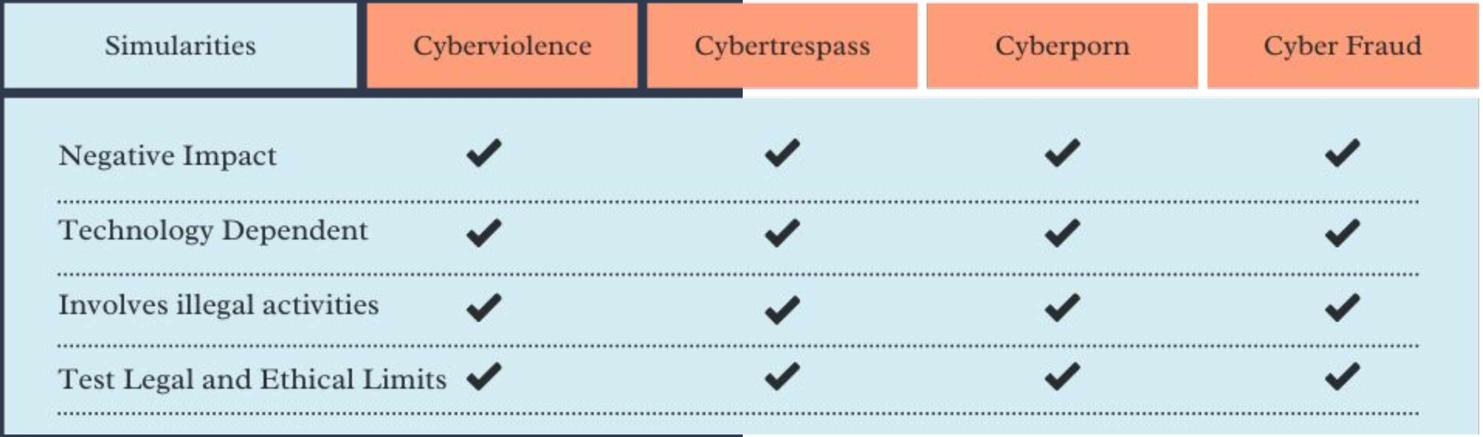
Fake websites

Category Comparisons

Similarities of the Categories

How are cyberviolence, cyber trespassing, cyberpornography and cyberfraud similar?

- ➔ **Impact on Victims:** All four categories of cybercrime can have a significant impact on victims, including but not limited to emotionally, psychologically, and/or financially.
- ➔ **Technological Dependence:** Rely on digital platforms for execution of the crimes
- ➔ **Illegal Activities:** Each category involves activities that are illegal and punishable under a variety of national and international laws that are in place to protect individual citizens and organizations.
- ➔ **Legal and Ethical Questions:** All four categories involve complex legal and ethical considerations that require nuanced regulation and law enforcement.

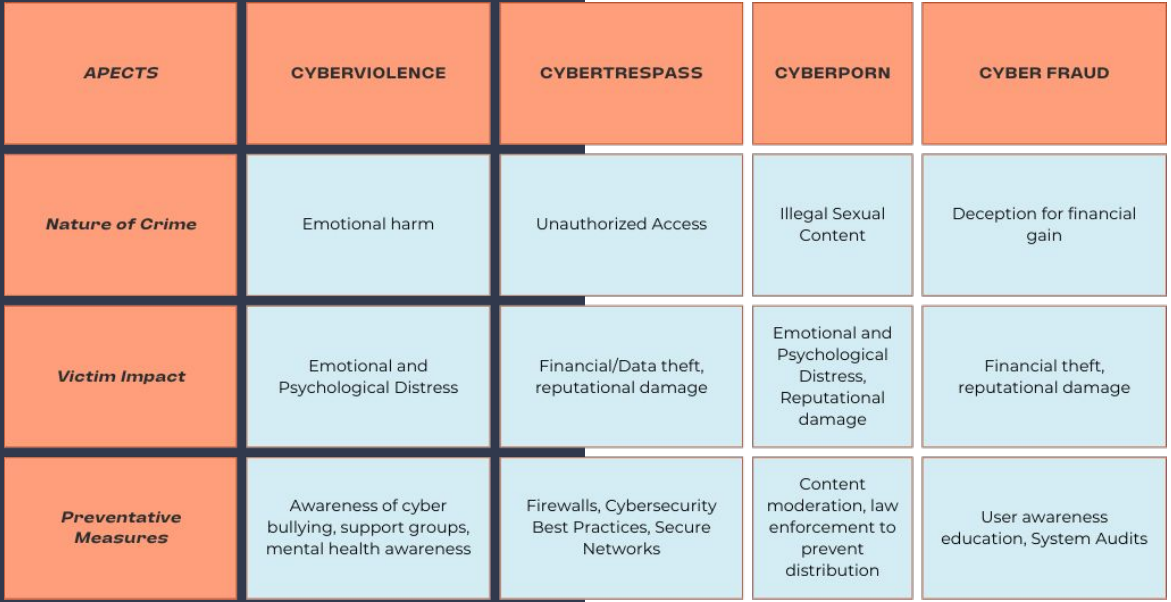


Simularities	Cyberviolence	Cybertrespass	Cyberporn	Cyber Fraud
Negative Impact	✓	✓	✓	✓
Technology Dependent	✓	✓	✓	✓
Involves illegal activities	✓	✓	✓	✓
Test Legal and Ethical Limits	✓	✓	✓	✓

Differences of the Categories

What distinguishes cyber fraud, cyberpornography, cyberviolence, and cybertrespassing from one another?

- ➔ Cyberviolence, cybertrespass, cyberpornography, and cyber fraud are distinct crimes that can cause emotional harm, unauthorized access, illegal sexual content, and financial deceit.
  - ◆ Victims of these crimes can suffer from emotional and psychological harm, financial theft, and reputational damage.
- ➔ Preventative measures are necessary for each crime, including mental health support systems, cybersecurity measures, content moderation, and law enforcement.
  - ◆ Cyberpornography and fraud require detection systems and education on common scams to minimize risk.



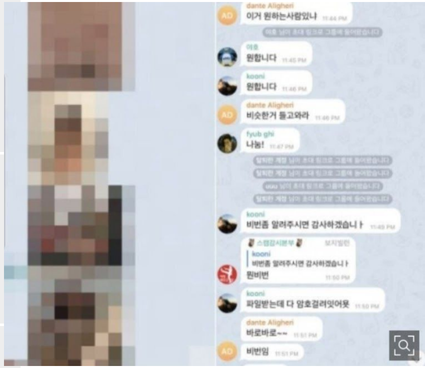
APECTS	**CYBERVIOLENCE**	**CYBERTRESPASS**	**CYBERPORN**	**CYBER FRAUD**
Nature of Crime	Emotional harm	Unauthorized Access	Illegal Sexual Content	Deception for financial gain
Victim Impact	Emotional and Psychological Distress	Financial/Data theft, reputational damage	Emotional and Psychological Distress, Reputational damage	Financial theft, reputational damage
Preventative Measures	Awareness of cyber bullying, support groups, mental health awareness	Firewalls, Cybersecurity Best Practices, Secure Networks	Content moderation, law enforcement to prevent distribution	User awareness education, System Audits

Recent Events of Cybercrime

The Nth Room

01 What is it?

The Nth Room was a set of private chat rooms in Korea on the popular site, Telegram. Victims, who were mostly women and children, were blackmailed into entertaining the individuals within them with dehumanizing content. Some were threatened, while others were promised fame. But all got stuck in the horrendous system, with no hope for escape.



dante Alighieri
이거 원하는사람있나 11:44 PM

이호 님이 초대 링크로 그룹에 들어왔습니다

이호
원합니다 11:45 PM

kooni
원합니다 11:46 PM

dante Alighieri
비슷한거 들고와라 11:46 PM

fyub ghi
나눔! 11:47 PM

탈퇴한 계정 님이 초대 링크로 그룹에 들어왔습니다

탈퇴한 계정 님이 초대 링크로 그룹에 들어왔습니다

uuu 님이 초대 링크로 그룹에 들어왔습니다

탈퇴한 계정 님이 초대 링크로 그룹에 들어왔습니다

kooni
비번좀 알려주시면 감사하겠습니ㅏ 11:49 PM

스팸감시본부 보지빌런
> kooni
> 비번좀 알려주시면 감사하겠습니ㅏ

뭔비번 11:50 PM

kooni
파일받는데 다 암호걸려잇어욧 11:50 PM

dante Alighieri
바로바로~~ 11:51 PM

비번임 11:51 PM

02 How did it work?

After coercing the victims into posting said content, it was then shared with paying customers. The Nth rooms were like a hierarchy, with the most expensive rooms having the most explicit content. Users would pay with cryptocurrency. Users could pay to “brand” their favorite victim with tattoos and scars. Some would even pay to gain access to the victim's address and attack them.

03 Outcome?

Tens of thousands of users within Korea alone had access to the Nth room. When the news broke, authorities arrested Baska, the ringleader, and sentenced him to life in prison. The individuals who paid to access the chat rooms were also pursued in order to hold them accountable for the abuse.

04 Social and cultural impact?

The Nth Room case led to stronger laws to protect victims and harsher penalties for online predators. It also raised global awareness about how encrypted platforms can be used for criminal activities, prompting debates about the need for better regulation of digital spaces.

The Nth Room:

In the Context of Cyberpornography

Cyberpornography: ***the illegal creation, distribution, or possession of pornography online*****.**

- This case fits cyberpornography because it involves the exploitation and nonconsensual collection and distribution of explicit content.
  - Many of the victims were minors.
  - Every victim was manipulated, threatened, and/or blackmailed into joining.
  - Some were even trafficked, being “sold” within those chat rooms.

- Under the Miller Test, the content from the Nth Room would pass as **obscene**. The content shared was sexually explicit, showed an explicit act of sex, and had no societal value beyond sexual consumption. Some of the content sold includes, but is not limited to:
  - Using nonsexual items in a sexual way
  - Branding themselves with knives, burnt objects, or tattooing
  - Consuming their own bodily waste
  - Having explicit relations with top-paying users

While pornography might be described as victimless crimes, the Nth Room scandal clearly demonstrates that such crimes do have victims. **The exploitation and abuse of women and minors refute the notion that there are no direct victims involved.**

Conclusion

Cybercrime can be divided into four primary categories: cyberviolence, cybertrespass, cyberpornography, and cyber fraud.

Recognizing these categories is essential for safeguarding both individuals and systems. As cyberpornography continues to evolve, it becomes increasingly important to remain vigilant and informed. By being aware and cautious, we can efficiently address cybercrime.

Ultimately, understanding these types allows us to better protect ourselves and our digital environments.

References

Cybersecurity & Infrastructure Security Agency. “Cybersecurity Resources.” *CISA* (2020). https://www.cisa.gov/.

Esguerra, V. (2024, August 30). Exploring the Nth Room: South Korea’s worst case of Digital Sexual Exploitation. The Mary Sue. https://www.themarysue.com/exploring-the-nth-room-south-koreas-worst-case-of-digital-sexual-exploitation/

Federal Bureau of Investigation. “Cyber Crime.” *FBI* (2024). https://www.fbi.gov/investigate/cyber

Graham, R.S., & Smith, '.K. (2024). Cybercrime and Digital Deviance (2nd ed.). Routledge. https://doi-org.proxy.lib.odu.edu/10.4324/9781003283256

Lee. (2024, July 29). The shocking nth room case: South Korea’s Dark Digital Crime scandal. DocumentKorea. https://dockorea.com/nth-room-case/

Wollert, Richard. (2012). The implications of recidivism research and clinical experience for assessing and treating federal child pornography offenders. http://www.ussc.gov/Legislative_and_Public_Affairs/Congressional_Testimony_and_Reports/Sex_Offense_Topics/201212_Federal_Child_Pornography_Offenses/index.cfm

The end.

Department of Sociology and Criminal Justice, Old Dominion University
CRJS/CYSE 310: Cybercrime: Foundations
Dr. Roderick Graham