

Cyber Sex Crimes: An Interdisciplinary Analysis of Legal, Psychological, Technological and Forensic Challenges

Jyh-Woei Lin

Department of Electrical Engineering, Southern Taiwan University of Science and Technology, Tainan, 710301, Taiwan,

 <https://orcid.org/0000-0001-6875-0172>

ABSTRACT

Cyber-sex crimes represent one of the fastest-growing forms of cybercrime, driven by the widespread adoption of the internet, social media, smartphones, encrypted communication platforms, and artificial intelligence (AI). These offenses include online grooming, sextortion, child sexual abuse material (CSAM), non-consensual dissemination of intimate images, cyber stalking, deepfake pornography, and technology-facilitated human trafficking. Unlike traditional sexual crimes, cyber sex crimes transcend geographical boundaries, allowing offenders to exploit victims anonymously and often repeatedly. Victims suffer severe psychological, social, and economic consequences, while law enforcement agencies face significant challenges in identifying perpetrators, collecting digital evidence, and prosecuting crimes across multiple jurisdictions. This paper examines cyber sex crimes from legal, criminological, psychological, technological, and forensic perspectives. It reviews the evolution of cyber-enabled sexual offending, analyzes offender motivations and victim vulnerabilities, discusses international legal frameworks, and explores emerging technological threats such as AI-generated pornography and encrypted communication. The paper argues that combating cyber sex crimes requires an integrated approach involving legal harmonization, digital forensic innovation, international cooperation, public education, victim-centered support services, and responsible technological governance.

KEYWORDS: Cyber Sex Crimes; Cybercrime; Sextortion; Child Sexual Abuse Material (CSAM); Deepfake Pornography; Legal Frameworks.

*Corresponding Author: Jyh-Woei Lin

1. INTRODUCTION

The digital revolution has transformed nearly every aspect of human interaction. Internet technologies, smartphones, social networking platforms, cloud computing, and artificial intelligence have dramatically expanded opportunities for communication, education, and commerce. However, these same technologies have also enabled new forms of criminal behavior. Among the most alarming developments is the rapid increase in cyber sex crimes (Gautam and Yadav, 2026) (**Figure.1**), which have become a significant concern for

governments, law enforcement agencies, educators, mental health professionals, and policymakers worldwide. Cyber sex crimes involve the use of digital technologies to facilitate sexual exploitation, abuse, harassment, coercion, or the production and dissemination of illegal sexual material. Unlike traditional sexual offenses, cyber sex crimes may occur without physical contact, allowing offenders to target victims across national borders while remaining anonymous. The digital environment enables offenders to communicate with multiple victims simultaneously, distribute illegal material instantaneously, and conceal their identities through encryption, virtual private networks (VPNs) (Ganesh et al., 2026), crypto currencies, and dark web services. The proliferation of social media platforms has significantly increased opportunities for offenders to identify and manipulate vulnerable individuals. Children and adolescents are particularly at risk because of their extensive online presence, limited awareness of digital risks, and developmental susceptibility to manipulation. Nevertheless, adults are also increasingly targeted through cyberstalking, sextortion, revenge pornography, identity theft, and AI-generated sexual images. Recent technological advances have further complicated the cyber sex crime landscape. Artificial intelligence now enables the creation of highly realistic synthetic pornography, commonly known as deepfake pornography (Räsänen, 2026), while encrypted messaging services complicate law enforcement investigations. Blockchain-based crypto currencies facilitate anonymous financial transactions associated with online sexual exploitation, and cloud storage allows illegal material to be distributed globally within seconds. Cyber sex crimes have profound consequences for victims. Psychological trauma frequently includes depression, anxiety, post-traumatic stress disorder (PTSD), social isolation, loss of employment, academic decline, and suicidal ideation. Unlike physical crimes, digital victimization often persists indefinitely because online content can be copied, archived, and redistributed repeatedly, resulting in continuous revictimization. The interdisciplinary nature of cyber sex crimes requires collaboration among legal scholars, criminologists, psychologists, computer scientists, forensic investigators, educators, and policymakers. This paper analyzes cyber sex crimes through these multiple perspectives to identify effective prevention strategies and propose future directions for research and policy development.

2. DEFINING CYBER SEX CRIMES

Cyber sex crimes refer to criminal acts involving sexual exploitation or abuse that are committed through digital technologies or facilitated by information and communication technologies (ICT). The Internet serves not only as a communication platform but also as an environment where offenders recruit victims, exchange illegal material, coordinate criminal activities, and evade law enforcement. Cyber sex crimes differ from conventional sexual offenses in several important ways: The offender and victim may never meet physically, Crimes frequently occur across multiple legal jurisdictions and digital evidence is often volatile and technically complex. Victimization may continue indefinitely through repeated online dissemination. Offenders frequently exploit anonymity technologies. Scholars generally classify cyber sex crimes into two categories: **(1)** Cyber-enabled sexual crimes, where traditional sexual offenses are facilitated by digital technologies (e.g., online grooming leading to physical abuse). **(2)** Cyber-dependent sexual crimes, which exist only because of digital technologies (e.g., AI-generated deepfake pornography or hacking webcams for sexual exploitation). Common examples include online grooming, child sexual abuse material (CSAM), sextortion, revenge pornography, non-consensual

dissemination of intimate images, cyberstalking, sexual harassment through electronic communication, deepfake pornography, live-streamed sexual abuse and technology-assisted human trafficking

3. MAJOR TYPES OF CYBER SEX CRIMES

3.1 Online Grooming

Online grooming involves establishing an emotional relationship with a child or vulnerable individual through digital communication to facilitate sexual exploitation. Offenders often pose as peers, gradually building trust before introducing sexual content or arranging offline meetings and social media platforms, gaming environments, and messaging applications have become common venues for grooming activities.

3.2 Child Sexual Abuse Material (CSAM)

Child sexual abuse material involves images or videos depicting the sexual abuse of minors. Modern cloud storage services, encrypted messaging platforms, peer-to-peer networks, and the dark web have significantly increased the global distribution of CSAM. Victims experience ongoing trauma because the material may remain accessible indefinitely.

3.3 Sextortion

Sextortion occurs when offenders obtain intimate images or videos and threaten to release them unless victims provide money, additional explicit material, or sexual favors. Offenders commonly exploit hacked accounts, social engineering, phishing attacks, or deception to obtain compromising images.

3.4 Non-Consensual Dissemination of Intimate Images

Commonly referred to as "revenge pornography," this offense involves sharing intimate images without the subject's consent. Although initially associated with former romantic partners, contemporary cases increasingly involve hacking, identity theft, or image manipulation rather than revenge motives.

3.5 Deepfake Pornography

Artificial intelligence enables the creation of realistic synthetic sexual images by superimposing an individual's face onto pornographic content. Victims may suffer reputational damage, emotional distress, employment consequences, and harassment despite never having participated in the depicted activities.

3.6 Cyberstalking

Cyberstalking involves repeated online harassment, surveillance, threats, or intimidation. Offenders may use GPS tracking, spyware, social media monitoring, or impersonation to intimidate victims over extended periods.

3.7 Live-Streamed Sexual Exploitation

The growth of live-streaming technology has enabled offenders to pay for real-time sexual abuse broadcasts, often involving children in economically disadvantaged regions. These crimes frequently involve organized

transnational criminal networks.

4. FACTORS CONTRIBUTING TO CYBER SEX CRIMES

Several interconnected factors contribute to the growth of cyber sex crimes technological Factors, internet anonymity, end-to-end encryption, cloud computing, crypto currency, artificial intelligence, virtual reality, dark web marketplaces, psychological Factors, sexual deviance, impulsivity, narcissism, Lack of empathy, internet addiction, compulsive sexual behavior, social factors, increased online interaction, weak parental supervision, social isolation, digital dependency, peer influence and economic Factors. Organized criminal groups increasingly exploit cyber sex crimes because they generate substantial profits while presenting relatively low risks compared with conventional organized crime.

5. IMPACT ON VICTIMS

Cyber sex crimes produce multidimensional harm Psychological Effects. Victims commonly experience depression, anxiety, PTSD, shame, self-blame, fear, Sleep disorders, suicidal thoughts and social Consequences. Victims may encounter cyber bullying, relationship breakdown, employment loss, academic decline, public humiliation, social isolation and financial Consequences. Victims frequently incur costs associated with legal proceedings, counseling, cybersecurity services, and identity restoration.

6. CHALLENGES FOR LAW ENFORCEMENT

Investigating cyber sex crimes presents unique obstacles Cross-border jurisdictional conflicts, Anonymous offenders, Encryption technologies, Large volumes of digital evidence, Rapid deletion of online content, Limited international cooperation and Resource constraints. Digital forensic investigators must preserve electronic evidence while maintaining chain-of-custody standards. Investigations often require collaboration among internet service providers, financial institutions, cybersecurity experts, and international policing organizations.

7. LEGAL RESPONSES

Many countries have strengthened legislation addressing cyber sex crimes by criminalizing online grooming, image-based sexual abuse, CSAM possession and distribution, and technology-facilitated exploitation. International cooperation is supported through treaties such as the Budapest Convention on Cybercrime and other regional agreements, though differences in national laws continue to hinder effective cross-border enforcement.

8. PREVENTION STRATEGIES

Effective prevention requires a multidisciplinary approach Comprehensive digital literacy education, Online safety programs for children and parents, AI-based detection of illegal content, Stronger cybersecurity practices, Improved victim reporting mechanisms, International legal cooperation, Public awareness campaigns and Trauma-informed victim support services. Technology companies also play a critical role by implementing content moderation systems, age verification mechanisms, and rapid response procedures for removing illegal material.

9. CONCLUSION

Cyber sex crimes have evolved into one of the most complex forms of transnational Cybercrime. Rapid technological innovation has expanded opportunities for offenders while simultaneously challenging traditional legal systems and investigative methods. The emergence of artificial intelligence, encrypted communications, cryptocurrencies, and digital platforms has fundamentally changed both the scale and sophistication of online sexual exploitation. Addressing cyber sex crimes requires more than criminal prosecution alone. Effective responses must integrate legal reform, international cooperation, advanced digital forensic capabilities, responsible technology governance, public education, and comprehensive support for victims. As digital technologies continue to evolve, governments, technology companies, researchers, and civil society must work collaboratively to ensure that innovation is accompanied by robust safeguards that protect human dignity, privacy, and fundamental rights. A comprehensive strategy that combines prevention, enforcement, technological innovation, and victim-centered policies offers the most promising path toward reducing cyber sex crimes and creating a safer digital environment for all users.

Acknowledgments:

The author is grateful to Southern Taiwan University of Science and Technology.

Data availability statement: Data sharing is not applicable (only appropriate if no new data is generated or the article describes entirely theoretical research)

Conflicts of interest: The author declares that there are no conflicts of interest.

Author Contributions: The author contributed to the conceptualization, writing, review and editing of this manuscript.

Funding statement: There is no funding "Not Applicable"

Compliance with ethical statements consisting of conflicts of interest Funding statement: There is no funding "Not Applicable"

Compliance with ethical statements consisting of conflicts of interest statements and informed consent

- (1) All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.
- (2) The author declares that there are no conflicts of interest.
- (3) Informed consent was obtained from all individual participants involved in the study.
- (4) This work does not include animals as subjects.

REFERENCES

1. Ganesh, V., Deshmukh, S. and Kotwal, J., (2026), Hybrid intrusion detection system using particle swarm optimization and neural networks for external threat detection, *Journal of Integrated Science and Technology*, Vol.14 (2), 1519, doi: 10.62110/sciencein.jist.2026.v14.1519.
2. Gautam, R. and Yadav, S., (2026), Psychological impact of cyber-crime on victims, *Current Psychology*, Vol.45, 240, doi: 10.1007/s12144-025-08873-x
3. Räsänen, J., (2026), OnlyFans and Deep Fake Porn – Can We Accept the Former but Condemn the Latter? *The New Bioethics*, Vol.32 (1), 55-65, doi: 10.1080/20502877.2025.2610910.

Cybersexual Crimes

Understanding, Impact, and Responses

Cybersexual crimes (also called online sexual crimes or technology-facilitated sexual offenses) are sexual offenses committed, facilitated, or amplified through digital technologies such as the internet, social media, smartphones, artificial intelligence, and online platforms. These crimes involve violations of sexual autonomy, privacy, dignity, or consent in digital environments.

1. COMMON FORMS OF CYBERSEXUAL CRIMES

- Non-Consensual Sharing of Intimate Images**
Also known as "revenge porn," involves distributing intimate photos or videos without consent.
- Online Sexual Harassment**
Includes unwanted sexual comments, messages, requests for sexual favors, or persistent online stalking.
- Grooming**
Building trust with a minor online for the purpose of sexual exploitation.
- Sextortion**
Threatening to share intimate images or information unless the victim provides money, more images, or other favors.
- Deepfake Sexual Abuse**
Using AI or editing tools to create realistic fake sexual images or videos of individuals without consent.
- Live Streaming Sexual Exploitation**
Forcing or coercing individuals to perform sexual acts on camera.
- Online Trafficking and Exploitation**
Using online platforms to recruit, transport, harbor, or exploit individuals for sexual purposes.

2. TECHNOLOGIES THAT FACILITATE THESE CRIMES

- Internet & Social Media**
(Anonymity, broad reach, easy sharing)
- Smartphones & Messaging Apps**
(Instant communication, hidden content)
- Artificial Intelligence & Deepfake Tools**
(Realistic manipulation, face swapping)
- Cloud Storage & File Sharing Platforms**
(Easy storage and anonymous distribution)
- Dark Web & Encrypted Platforms**
(Anonymity, illegal content markets)

3. IMPACTS ON VICTIMS

- Psychological Harm:** anxiety, depression, PTSD, shame
- Emotional & Social Harm:** damaged relationships, social isolation
- Loss of Privacy & Dignity:** long-term violation of autonomy
- Educational & Career Impact:** decreased performance, reputation damage
- Risk of Revictimization:** content can spread and resurface

4. WHY THESE CRIMES ARE GROWING

- Increased digital connectivity and online activity
- Anonymity and impunity of perpetrators
- Easy access to tools for image/video manipulation
- Lack of digital literacy and awareness
- Gaps in laws and slow legal responses
- Victim-blaming culture and lack of support systems

5. LEGAL AND POLICY RESPONSES

- Enact and enforce laws that criminalize cybersexual offenses
- Strengthen cross-border cooperation
- Mandate platform accountability and content takedown mechanisms
- Protect digital evidence and victim privacy
- Provide victim-centered support services

6. PREVENTION AND AWARENESS

- Promote digital literacy and consent education
- Encourage safe online behavior
- Raise awareness about reporting channels
- Engage tech companies in ethical design and monitoring
- Support survivors and reduce stigma

CONCLUSION

Cybersexual crimes are a growing global crisis that violates fundamental human rights. Addressing them requires a multi-stakeholder approach involving government, technology companies, educators, law enforcement, and civil society to create safer digital spaces for all, especially the most vulnerable.

REMEMBER

It is never the victim's fault. Consent exists online, too.

Figure.1 Cyber sex crimes (also called online sexual crimes or technology-facilitated sexual offenses) are sexual offenses committed, facilitated, or amplified through digital technologies such as the internet, social media, smartphones, artificial intelligence, and online platforms. These crimes involve violations of sexual autonomy, privacy, dignity, or consent in digital environments.