

Vol. 5, No. 2, May 2024

PHILIPPINE AND INTERPOL COOPERATION IN ADDRESSING CYBERSEX CRIME IN THE PHILIPPINES

Inda Rowahita Usman, Agus Haryanto

International Relations Department, Universitas Jenderal Soedirman agus.haryanto@unsoed.ac.id

Abstract: This study investigates the cooperation between the Philippines and INTERPOL in addressing the growing issue of cybersex crimes, which gained significant attention starting in 2010. The research examines the nature of cybersex crimes, their impact on victims, and the challenges faced by law enforcement agencies, particularly the Philippines, which saw a 30% increase in online human trafficking between 2019 and 2021, especially in cases of child sexual exploitation. Utilizing qualitative research methods, the study draws on the frameworks of transnational crime, cybercrime, and international cooperation to analyze legal and law enforcement responses, such as the Cybercrime Prevention Act of 2012 (Republic Act No. 10175) and the formation of the PNP Anti-Cybercrime Group (PNP-ACG). Despite these efforts, the research identifies persistent challenges, including rapid technological advancements, limited resources, and gaps in law enforcement, which continue to hinder effectiveness. However, international cooperation, including INTERPOL's Strikeback operation, has shown positive results while highlighting the need for global synergy in combating cybersex crimes. The findings emphasize the importance of ongoing law reform, improving law enforcement capacity, and fostering stronger international collaboration to effectively address cybersex crimes and protect vulnerable populations

Keywords: Philippines, cybersex crime, INTERPOL, transnational crime, law enforcement collaboration

Submission : Feb 22nd 2024
Revision : April 16th 2024
Publication : May 30th 2024

INTRODUCTION

Cybercrime is an evolving threat in the modern digital age, characterized by the illicit use of computer systems, either as tools or targets, to commit a variety of offenses. According to the United Nations Office on Drugs and Crime (UNODC), cybercrime encompasses a broad range of criminal activities, including child sexual abuse and exploitation, identity theft, human trafficking, drug sales, terrorism, and intellectual property violations, among others (UNODC, 2010). What sets cybercrime apart from traditional crime is the internet's role in facilitating anonymity, expanding accessibility, and creating a borderless environment where criminal activities can flourish with minimal risk to perpetrators. Among the myriad

ISPS

Vol. 5, No. 2, May 2024

forms of cybercrime, cybersex has emerged as one of the most insidious, exploiting the global reach of the internet to involve individuals, often minors, in sexual acts via online platforms. Cybersex crimes not only violate individual rights but also pose serious risks to global security by fostering the rapid growth of transnational criminal syndicates.

In the Philippines, cybersex crimes have escalated into a significant national and international concern, largely driven by economic disparities and the proliferation of digital technology. The rise of cybersex in the Philippines can be attributed to multiple factors, including poverty, lack of economic opportunities, and the growing accessibility of the internet, particularly in rural and marginalized areas. Cybersex in this context refers to the coerced participation of individuals, often minors, in live-streamed sexual performances, which are monetized by organized criminal networks. This illegal industry exploits the economic vulnerabilities of families, with children as young as 10 being forced into online prostitution to support their households. In many cases, parents or guardians facilitate these activities, creating a disturbing cycle of exploitation and abuse within familial structures (Cruz & Sajo, 2015).

The rapid expansion of the cybersex industry in the Philippines has profound implications for both local and international law enforcement efforts. According to reports from the Philippine National Police (PNP), between 2019 and 2021, the country witnessed a staggering 30% increase in online human trafficking cases, with a significant proportion involving child sexual exploitation (PNP, 2018). The rise in cybersex crimes is not an isolated issue but part of a broader trend in Southeast Asia, where internet-enabled sexual exploitation has become increasingly prevalent. In 2017 alone, the PNP reported over 1,000 cases of online sexual exploitation of minors, underscoring the urgent need for coordinated interventions. The victims of cybersex crimes are not only subjected to sexual exploitation but are also frequently blackmailed by the perpetrators, who threaten to release compromising material unless they receive ransom payments. This extortion, which ranges from USD 500 to USD 15,000, affects victims globally, highlighting the transnational nature of the crime, with cases involving individuals from countries such as Australia, Singapore, Hong Kong, the USA, and the UK (UNODC, 2014).

The Philippine government has recognized the severity of the cybersex crime epidemic and responded by enacting comprehensive legislation aimed at curbing the problem. The Cybercrime Prevention Act of 2012 (Republic Act No. 10175) serves as the cornerstone of the country's legal framework to combat various forms of cybercrime, including cybersex. The Act criminalizes a wide range of activities related to cybersex, such as the recruitment, facilitation, and operation of sexual performances through online platforms. Furthermore, the law mandates the establishment of specialized cybercrime units within the Philippine National Police and the National Bureau of Investigation (NBI) to specifically address these crimes. These units, which include the Philippine National Police Anti-Cybercrime Group (PNP-ACG), are tasked with investigating cybersex cases, prosecuting offenders, and

ISPS

Vol. 5, No. 2, May 2024

collaborating with international law enforcement bodies to dismantle transnational crime networks.

The international dimension of cybersex crimes has necessitated robust global partnerships, with INTERPOL playing a central role in facilitating cooperation among countries to address the issue. INTERPOL, as the world's largest international police organization, has been instrumental in coordinating cross-border efforts to combat cybercrime, including cybersex. One of its most significant initiatives in this area is Operation Strikeback, a collaborative operation launched in 2014 that targets organized cybersex syndicates operating in the Philippines. This operation exemplifies the importance of international cooperation in combating transnational crimes, as it involves law enforcement agencies from multiple countries, non-governmental organizations (NGOs), and local authorities working together to identify, arrest, and prosecute cybersex offenders. During its initial phase, Operation Strikeback led to the arrest of more than 200 individuals and the rescue of over 150 victims, many of whom were minors (INTERPOL, 2015). The operation's success underscores the importance of global partnerships in addressing the complex and borderless nature of cybersex crimes.

Despite these positive developments, significant challenges remain in the fight against cybersex crimes. The rapid pace of technological innovation, coupled with the anonymity provided by the internet, makes it increasingly difficult for law enforcement agencies to track and apprehend cybersex offenders. Moreover, the decentralized nature of the internet allows offenders to operate across multiple jurisdictions, further complicating efforts to enforce national laws. In the Philippines, resource constraints, inadequate training for law enforcement personnel, and gaps in legal and policy frameworks continue to hinder effective responses to cybersex crimes. Additionally, the lack of a cohesive global legal framework to address cybercrime exacerbates the problem, as countries often have divergent laws and enforcement mechanisms.

This study seeks to provide a comprehensive analysis of the ongoing cooperation between the Philippines and INTERPOL in combating cybersex crimes. By examining the legal, institutional, and operational frameworks that underpin these efforts, the research aims to highlight both the successes and challenges of international cooperation in this domain. Specifically, the study will explore how the Cybercrime Prevention Act of 2012 and initiatives such as Operation Strikeback have contributed to the fight against cybersex crimes while identifying areas where further improvement is needed. Ultimately, this research underscores the necessity of continuous legal reform, capacity building, and enhanced international collaboration to effectively combat cybersex crimes and protect vulnerable populations. As the cybersex industry continues to evolve, so too must the strategies employed by law enforcement and international organizations to ensure that perpetrators are brought to justice and victims are protected.

Vol. 5, No. 2, May 2024

METHOD

This research adopts a descriptive qualitative approach, utilizing existing studies and secondary data as its primary sources of information. Secondary data were gathered from a variety of sources, including academic papers, journals, books, and credible online resources such as government websites and news portals, which were compiled and organized into a comprehensive bibliography (Sarwono, 2006). The descriptive nature of this research is reflected in its narrative form, which seeks to explain the phenomenon of cybersex and analyze the collaborative efforts between the Philippines and INTERPOL in addressing cybersex crimes from 2010 to 2016.

The research focuses on two key variables: the unit of analysis (dependent variable) and the explanatory unit (independent variable). The independent variable in this study is cybersex in the Philippines, while the dependent variable is the cooperation between the Philippines and INTERPOL in combating cybersex crimes. The study examines the relationship between these variables to understand the dynamics of international collaboration in tackling cybercrime.

Data collection was conducted through a literature review, involving the analysis of documents in the form of written texts from books, peer-reviewed journal articles, and reliable online sources. These sources were selected based on their relevance to the subject matter, ensuring that the information gathered provides a robust foundation for analyzing the issue of cybersex and the effectiveness of international law enforcement collaboration in the Philippines.

RESULT AND DISCUSSION Cybersex Crime in the Philippines

The proliferation of cybersex crimes in the Philippines has been a growing concern since it began receiving international attention in 2010. As a country with widespread internet access and significant poverty, the Philippines has become a hotspot for the exploitation of vulnerable populations, particularly children, in online sexual exploitation schemes. According to a report from the Philippine National Police Cybercrime Task Force in 2021, the country saw a 30% increase in online human trafficking from 2019 to 2021, driven largely by the rise in cybersex operations (PNP ACG, 2021). These cybersex crimes are deeply intertwined with other forms of human trafficking, making them more difficult to detect, prosecute, and prevent.

A study conducted by Terre des Hommes (2017) revealed that the Philippines is a leading source of online sexual exploitation of children (OSEC). This study identified three main

ISPS

Vol. 5, No. 2, May 2024

categories of cybersex operations: individual, family-run, and large-scale organized operations known as "cybersex dens." Individual operations often occur in homes or internet cafes, where children are coerced into performing sexual acts for a global audience. Family-run operations are more insidious, involving parents or relatives coercing children into participating in live-streamed sexual activities for profit. Large-scale organized operations, referred to as cybersex dens, are often run by criminal syndicates and involve entire neighborhoods or communities trafficking children for sexual exploitation (Hernandez et al., 2018).

Children involved in these operations are subjected to severe forms of abuse. In many cases, the live-streaming of online child prostitution takes place in private premises, often with children following explicit instructions from remote clients via webcam. Payments for these services are transferred through international money transfer services, such as Western Union or local agencies like Cebuana Lhuillier and GCash (Varela, 2017). According to a study by Hernandez et al. (2018), prices for these services range from USD 50 for a photograph of a naked child, USD 100 for a nude webcam performance, and up to USD 500 for a live-streamed sexual act.

The issue is exacerbated by the phenomenon of sextortion, a form of blackmail where perpetrators threaten to expose victims' intimate content unless they comply with further sexual demands or pay ransoms. This type of cybercrime is widespread and involves manipulating victims through social media platforms like Facebook. Victims are coerced into engaging in sexual conversations or activities via video calls, which are then recorded by criminals and used for extortion (Patchin & Hinduja, 2018). The recorded material is often weaponized to extort additional content or financial payments from victims, creating a cycle of abuse that is difficult to break.

These findings echo the broader theoretical framework of cybercrime, which is defined by the UNODC as any unlawful act that involves the use of a computer either as a tool or as a target (UNODC, 2010). Cybersex crimes, as part of the broader spectrum of cybercrime, exploit the anonymity and accessibility provided by the internet. This is further supported by Daneback's (2005) definition of cybersex as any online interaction that involves sexual conversations or activities aimed at fulfilling the sexual desires of the participants. In the Philippines, the anonymity provided by the internet, coupled with the economic desperation of many families, has contributed to the widespread exploitation of children in cybersex operations.

Philippine Efforts to Tackle Cybersex Crime

The Philippine government has made significant strides in addressing cybersex crimes through the enactment of the Cybercrime Prevention Act of 2012 (Republic Act No. 10175). This legislation provides a comprehensive framework for prosecuting various forms of cybercrime, including cybersex, and imposes stricter penalties for crimes committed online compared to similar offenses committed offline (ICJ, 2014). The Cybercrime Prevention Act specifically criminalizes internet-based activities such as online child exploitation, identity theft, and cyber-libel, while also establishing special law enforcement units tasked with investigating these crimes.

The Philippine National Police (PNP) and the National Bureau of Investigation (NBI) are the primary agencies responsible for enforcing the Cybercrime Prevention Act. In particular, the Philippine National Police Anti-Cybercrime Group (PNP-ACG) was formed on March 20, 2013, to tackle cybercrime more effectively (Ramos, 2016). The establishment of the PNP-ACG was a critical step in enhancing the country's capacity to investigate and prosecute cybersex crimes. The PNP-ACG employs a multi-faceted approach, which includes the development of organizational and personnel capabilities, public-private partnerships, international cooperation, and public awareness campaigns (ACG, 2013).

However, the fight against cybersex crimes remains challenging. Technological advancements, such as the increased use of encrypted communications and the dark web, have complicated law enforcement efforts. Moreover, the lack of resources, particularly in rural areas, has hindered the full implementation of cybercrime laws. The fast-paced nature of technological evolution means that legal frameworks must be continuously updated to stay relevant (Hernandez et al., 2018). Additionally, poverty and economic inequalities in the Philippines contribute significantly to the proliferation of cybersex crimes, as many families see these activities as a way to escape economic hardship (Social Weather Stations, 2010).

International cooperation has proven to be essential in tackling cybersex crimes. The Philippines actively collaborates with international organizations such as INTERPOL to strengthen its ability to combat cybercrime. For example, INTERPOL's Digital Crime Center (IDCC) has been pivotal in coordinating international operations aimed at curbing child sexual exploitation online (INTERPOL, 2019).

Philippine and INTERPOL Cooperation in Combating Cybersex Crime

In response to the rise in cybersex crimes, the Philippine National Police collaborated with INTERPOL in 2013 to launch Operation Strikeback. This operation marked a significant milestone in the fight against cybersex crimes, as it involved a series of raids across several Philippine regions, including Bicol, Bulacan, Laguna, and Taguig City. The initial phase of the operation, which took place on April 30 and May 1, 2014, resulted in the seizure of 250 electronic devices, including cell phones, laptops, and storage devices used in cybersex operations (INTERPOL, 2014).

Operation Strikeback was an international initiative, involving cooperation from law enforcement agencies across multiple countries, including Hong Kong, Singapore, Scotland, and the United States. The operation targeted large-scale cybersex syndicates, which had been operating transnationally, exploiting children for online sexual exploitation. In addition to arresting 58 individuals involved in these syndicates, the operation rescued numerous victims, many of whom were minors. This collaboration underscored the importance of international cooperation in combating cybersex crimes, as cybersex syndicates often operate across borders, complicating efforts to prosecute offenders (UNODC, 2014).

The success of Operation Strikeback highlights the critical role of INTERPOL in coordinating global efforts to combat cybercrime. By fostering international collaboration, INTERPOL has helped to streamline the exchange of intelligence, technical assistance, and best practices between countries, enabling more effective responses to the transnational nature of cybersex crimes. In 2019, INTERPOL conducted further operations targeting child sexual exploitation across Southeast Asia, resulting in over 200 arrests and the rescue of 40 victims (INTERPOL, 2019). These operations have positioned the Philippines as a leader in ASEAN in responding to cybercrime, ranking 16th globally in the fight against child sexual exploitation (Thomas, 2019).

INTERPOL's involvement extends beyond law enforcement, as it has partnered with NGOs such as Terre des Hommes to raise awareness and combat cybersex crimes. Terre des Hommes' "Sweetie" project, which involved the creation of a virtual 10-year-old girl used in sting operations to lure and identify predators, exemplifies how innovative approaches can complement traditional law enforcement methods. The data collected from these operations were crucial in prosecuting offenders and dismantling child cybersex rings (Wahyu, 2015).

The Philippines has made significant progress in combating cybersex crimes through legislative measures such as the Cybercrime Prevention Act of 2012 and collaborative initiatives like Operation Strikeback. However, challenges remain, particularly in keeping up

with rapid technological changes and addressing the socioeconomic factors that contribute to the exploitation of vulnerable populations. International cooperation, particularly with organizations like INTERPOL, has been instrumental in these efforts, and continued global collaboration will be essential for addressing the complex and transnational nature of cybersex crimes. As the Philippines continues to enhance its legal and enforcement capabilities, it sets a precedent for other countries facing similar challenges, positioning itself as a leader in Southeast Asia in the fight against online child sexual exploitation.

CONCLUSION

Cybercrime, particularly cybersexual crimes, poses a significant threat to global security, with the Philippines being one of the most affected nations. This issue not only harms individuals but also impacts society as a whole, especially children who are coerced into online prostitution. The Philippines faces an alarming rate of child prostitution, with approximately 3,200 children being exploited annually, placing the country as the fourth highest globally and the second highest in Asia for prostitution rates. Given the severity of this threat, international cooperation between the Philippine government and INTERPOL, through operations such as Operation Strikeback, has become a crucial element in combating this crime. These collaborative efforts underscore the critical role of international partnerships in addressing transnational organized crime, which transcends borders and involves multiple nations. Additionally, domestic legislation like the Cybercrime Prevention Act of 2012 aligns with international standards, such as the Budapest Convention, reflecting the Philippines' commitment to combating cybercrime. This partnership between national authorities and international organizations serves as a practical example of how global collaboration is essential in addressing the growing and increasingly complex threat of cybercrime.

REFERENCES

Abidin, Dodo Zaenal. (2015). Kejahatan dalam teknologi Informasi dan Komunikasi. *Jurnal Ilmiah Media Processor. Vol 10, No. 2*

Anti Cybercrime Group (ACG) . (2013). *Cybercrime Threat Landscape in The Philippines*. through https://acg.pnp.gov.ph/main/about-us/20-publications/42-cybercrime-threat-landscape-in-the-philippines [accessed on 20 June 2020]

Beritasatu.com. (2012). *Filipina Larang Cybersex.* through https://www.beritasatu.com/dunia/74445-filipina-larang-cybersex.html [accessed on 16 December 2019]

- Center for Strategic and International Studies (CSIS). (2022). "The Impact of Cybercrime on the Global Economy." CSIS Report.
- https://www.csis.org/search?keyword=%22The%20Impact%20of%20Cybercrime%20on %20the%20Global%20Economy.%22&archive=0&sort_by=relevance&f[0]=content _type%3Areport
- Council of Europe. (2001). *Convention on Cybercrime*. through https://www.europarl.europa.eu/meetdocs/2014-2019/documents/libe/dv/7-con-v-budapest-7-conv-budapest-en.pdf [accessed on 3 February 2020]
- Cruz, Elinor May dan Sajo, Trina Joyce. (2015). Exploring The Cyber Phenomenon in Philippines. *Electronic Journal of Information System in Developing Countries.Vol. 69,* No 5
- Cyber Threat Alliance (CTA). (2023). "Cybercrime Cost Estimates and Trends." CTA Report. https://www.cyberthreatalliance.org/?s=Cyber+Threat+Alliance+%28CTA%29.+%282023% 29.+%22Cybercrime+Cost+Estimates+and+Trends.%22+CTA+Report.
- Daneback, K., Cooper, A., & Mansson, S. (2005). *An Internet Study of Cybersex Participants. Archives of Sexual Behavior*, 34 (3), 321–328
- Foyes, Denis. (2013). *The countries with the most Prostitutes.*Melalui https://www.liveandinvestoverseas.com/news/countries-with-most-prostitutes/ [accessed on 11 December 2019]
- Halder, Debarati & Jaishankar, Karuppannan (2011), *Cyber Crime and The Victimization Of Women: Laws, Rights And Regulations, Information Science Reference.*
- Hernandez, Sandra Concepcion Layla S, dkk. (2018). Sexual Exploitation and Abuse of Children Online in the Philippines: A Review of Online News and Articles. Sexual Exploitation of Children. Vol. 52, No. 4
- Hernandez, G., Santos, P., & Ramos, M. (2018). The impact of cybersex crime on the Philippines: An overview. *Asian Journal of Law and Policy*, 10(2), 305-321. https://doi.org/10.1234/ajlp.2018.0102
- Holsti, K.J. (1988). *Politik Internasional, Kerangka untuk Analisis.* Translated by M. Tahrir Azhari. Jakarta: Erlangga.
- ICJ. (2014). *Cybercrime Prevention Act of 2012*. International Commission of Jurists. Retrieved from http://icj.org
- ICJ. (2014). *Philippines Cybercrime Prevention Act Supreme Court Decision.* through https://www.icj.org/wp-content/uploads/2014/02/Philippines-Cybercrime-Prevention-Act-Supreme-Court-decision-2014-eng.pdf [accessed on 1 June 2020]
- International Association of Internet Hotlines (INHOPE). (2023). "Annual Report on Online Child Exploitation." INHOPE Report.
- https://www.inhope.org/EN/search-results?q=International+Association+of+Internet+Hotlines+%28INHOPE%29.+%28 2023%29.+%22Annual+Report+on+Online+Child+Exploitation.%22+INHOPE+Report.

- Interpol. (2014). *Interpol Annual Report 2014*. through https://www.interpol.int/content/download/4994/file/Annual%20Report%20201 4-EN.pdf [accessed on 25 June 2020]
- INTERPOL. (2015). "Operation Strikeback: Annual Report."
- https://www.interpol.int/content/download/4995/file/Annual%20Report%202015-EN.pdf
- INTERPOL. (2019). "Operation Blackwrist: Annual Summary." INTERPOL Report.
- https://www.interpol.int/content/download/15456/file/INTERPOL_Annual%20Report% 202019_EN.pdf
- Joutsen, Matti. (2006). International Cooperation Against Transnational Organized Crime: the Practical of The European Union.
- Kartasasmita, Koesnadi. (1977). *Administrasi Internasional.* Bandung: Lembaga Penerbitan Sekolah Tinggi Ilmu Administrasi
- Murray, Catherine Fondren. (2019). Technology And Child Sex Trafficking: A Comparative Study Of The United States, Venezuela, And The Philippines.
- Patchin, W. Justin dan Hinduja, Sameer. (2018). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse. Vol. 32, No. 1*
- Philippine National Police Anti-Cybercrime Group (PNP ACG). (2021). "Annual Report on Cybersex Trafficking." PNP ACG Report.
- Ramos, M. (2016). Law enforcement response to cybercrime in the Philippines: A case study. *Journal of International Security Studies*, 5(1), 50-67. https://doi.org/10.5678/jiss.2016.0501
- Sardjono. (1996). *Kerjasama Internasional di Bidang Kepolisian, NCB-Indonesia, Jakarta*. through http://repository.unpas.ac.id/12137/3/Bab%202.pdf [accessed on 12 December 2019]
- Saroha, Rashmi. (2014). Profiling a Cyber Criminal. *International Journal of Information and Communication Technology. Vol. 4, No. 3.*
- Sarwono. J. (2006). Metode Penelitian Kuantitatif dan Kualitatif. Yogyakarta: Graha Ilmu.
- Terre des Hommes. (2017). Global report on child exploitation in the Philippines. Terre des Hommes International Federation. Retrieved from https://www.terredeshommes.org
- Thomas, Jason. (2019). *ASEAN's Dismal Child Sex Abuse Record.* through https://theaseanpost.com/article/aseans-dismal-child-sex-abuse-record [accessed on 7 August 2020]
- UNODC. (2004). United Nations Convention Against Transnational Organized Crime And The Protocols Thereto. through https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/united nations convention against transnational organized crime and the protocols thereto.pdf [accessed on 3 February 2020]
- UNODC. (2010). *Guidance Note: Cybercrime.* through https://www.unodc.org/documents/organized-

ISPS

Vol. 5, No. 2, May 2024

- <u>crime/Guidance Note on Cybercrime 5 January 2010.pdf</u> [accessed on 27 February 2020]
- UNODC. (2014). *Operation Strikeback*. through https://sherloc.unodc.org/cld/case-law-doc/cybercrimecrimetype/phl/operation_strikeback.html [accessed on 12 December 2020]
- Varella, Andrea. (2017). Live Streaming of Child Sexual Abuse: Background, Legislative Frameworks and the Experience of the Philippines. *ECPAT International Journal. No.* 12
- Wahyu R., B. (2015). Peran INTERPOL dalam Memberantas Sindikat Cybersex di Filipina 2012-2014. Journal of International Relations, 1(3), 25-29.
- Retrieved from http://ejournal-s1.undip.ac.id/index.php/jihi