International Journal of Global Community
Volume V No.1 (March), 2022

The Role of Interpol in the Settlement of Cybercrime Cases under the Budapest Convention on Cybercrimes

Dirga Agung

Faculty of Law, Atma Jaya University, Makassar, Indonesia
E-mail: dirgagunk88@gmail.com

Abstract

Interpol is an international police organization that has the main function of information sharing regarding transnational and international crimes between its representatives in member countries. Constitution of ICPO-INTERPOL indicates that one of its aims is to ensure and promote the widest possible mutual assistance between all police authorities within the legal boundaries that exist in various countries and in the spirit of 'universal declaration of human rights'. The purpose of this article is to explore the effect of the Budapest Convention on the performance of Interpol in the fight against cybercrime cases. The Budapest Convention on Cybercrimes is an agreement based on an international decision to enhance state cooperation in dealing with cybercrime. In addition, this paper highlights the point that Interpol's arrangements as stated in the Budapest Convention are for both international treaty participants and non-international treaty participants. The results indicate that Interpol's performance in resolving cybercrime cases has been improved by the Budapest Convention on Cybercrimes.

Keywords: Interpol's role, Budapest Convention, Cybercrime.

Introduction

Present day, cybercrime is a crime that is very widespread because technology has become a part of life, as almost all daily human activities use technology. Cybercriminals take advantage of the above fact to commit various cybercrimes, leading to the huge losses on the part of victims. According to Girasa, cybercrime is an activity that uses computer technology as the main component. Tavani, on the other hand, defined cybercrime as a crime where criminal acts can only be carried out using cyber technology and occur in the cyber world.

Cybercrime, or computer-based crime, is a crime involving computers and networks (Moore, R., 2005). Computers are used to commit crimes, and the aim of perpetrators of crimes that take place in cyberspace is to profit from the act, just like physical crimes (Warren, et al, 2002: 392). A more detailed definition of cybercrime is as follows (Halder et al, 2011):

> An offense committed against an individual or group of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm either directly or indirectly, using modern telecommunications networks such as the Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth / SMS / MMS).

Further, computer fraud is a dishonest misrepresentation of facts intended to deceive someone into taking an action that would cause loss. In this context, the fraud is carried out by altering in an unauthorized way. It involves changing data, entering false data, entering unauthorized instructions or using an unauthorized process. It's also stealing output to hide unauthorized transactions, and changing or deleting stored data. Other forms of fraud can be facilitated using computer systems, including bank fraud, card fraud, identity theft, extortion and theft of confidential information. Many internet scams are based on phishing and social engineering, and the targets are usually consumers and business people.

Since the individual is the main target of cybercrime, the computer can be considered as a tool rather than a target. These crimes generally lack technical expertise. Human weaknesses are generally exploited. The damage done is mostly psychological and intangible, making legal action against this variant of crime more difficult. The elements of cybercrimes have existed for centuries in the offline world. Fraud, theft, and similar crimes were in existence even before the development of high-tech equipment.

The same criminals have been simply given tools that increase their potential to successfully defraud victims and make them even more difficult to track down and catch. Other computer network crimes include:

a. Fraud and identity theft (these are increasingly using hacking or phishing malware, making them examples of computer crime "as a target" and "computers as a tool").
b. Information warfare.
c. Phishing scams.
d. Spam.
e. Pornography, including harassment and threats.
f. Sending unsolicited bulk emails for commercial purposes (spam) is illegal in some jurisdictions. Phishing is mostly spread via email. Phishing emails may contain links to other websites affected by malware or may contain links to fake online banking or other websites used to steal personal account information.

The 2001 Budapest Convention on Cybercrimes regulates the formulation of criminal policy in order to protect the public from cybercrime and to increase cooperation between countries in dealing with such crime. Even though the convention was organized by the European Union, this international agreement is also open to non-European countries. A joint Europol-INTERPOL cybercrime has built with a call to develop innovative policing solutions to boost cybercrime investigations and help countries exploit digital evidence. Interpol involvement is a form of role that stipulated in Article 27 pragraph (9) Budapest Convention.

The International Criminal Police Organization (ICPO-Interpol) is an international law enforcement agency that plays a role in overcoming the problems of crime and violations of international law. Its duties include tackling and eradicating crimes that cross national borders. ICPO-Interpol coordinates cooperation among its international offices, including the National Central Bureau (NCB-Interpol) of each member country, by ensuring effective exchange of data and information and providing investigative assistance services. The transborder nature of cybercrime is a cause for serious concern among countries. If left unchecked, cybercrime will continue to increase and criminals would not be brought to justice to serve as a deterrent to others. This will clearly threaten the security of the international community (Widyawati, 2014: 132; Christien et al, 2021: 387).

Based on Article 2 of the Constitution of ICPO-INTERPOL, one of its aims is to ensure and promote the widest possible mutual assistance between all police authorities within the legal boundaries that exist in various countries and in the spirit of the universal declaration of human rights. On the second aim, constitution stipulated that Interpol “To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes”.

Due to the existence of cybercrimes as “extraordinary crimes” in various countries, including countries that are members of Interpol, it is necessary to take firm action against cybercriminals, who disrupt the security of citizens. In order to realize this, the Budapest Convention was held in Budapest-Hungary in 2001. This

study tries to describe the role of Interpol in accordance with Budapest Convention regulation.

Methodology

The research method used is normative legal research, which is carried out by examining library materials or secondary data as the basis for research. The data is obtained by searching for regulations related to the problems to be discussed. Thereafter, the legal materials that have been collected are analyzed qualitatively, which involves arranging them systematically based on legal disciplines to achieve clarity on the issues to be discussed.

Result and Discussion

Interpol's Role in Budapest Convention

The Budapest Convention consists of four chapters as follows: Chapter I deals with definitions and terminology; Chapter II focuses on actions to be taken at the national level of member states; Chapter III refers to international cooperation; and Chapter IV gives the concluding provisions. Based on the provisions of Chapter II, countries that ratify this cybercrime convention will have an obligation to harmonize their criminal law, both materially and formally, according to the predetermined scope. This means that there will be several additions to the criminal law for participating countries that have not included cybercrime in their national criminal law.

The forms of cybercrimes contained in the European Convention on Cybercrime are as follows:

1. *Illegal Content* is an activity that involves entering harmful content that violates the law and disturbs public order into the internet.
2. *Illegal Access* is accessing a computer system without permission from the owner, including basic violations of dangerous threats from attacks on data security and computer systems.
3. *Illegal Interception* is the activity of capturing or listening to transmissions and broadcasts without permission, more precisely known as eavesdropping.
4. *Data Interference* is the destruction of data without permission. Provisions that designate destruction of data as a criminal act aim to provide the same level of protection for computer data and computer programs as that of tangible objects. For example, entering malicious codes, viruses, and Trojan horses into a computer system is a violation according to the provisions of this article.
5. *System Interference* is an activity carried out by entering, disseminating, deleting, or hiding computer data so that it interferes with the existing system.

6. *Misuse of Device* is misusing equipment; the tool in question may be hardware or software that has been modified to gain access to a computer or computer network.
7. *Computer Related Offences*: Forgery and fraud are criminal activities related to computers.
8. *Content Related Offences*: Being in possession of child pornographic materials is an offence.
9. *Offences Related of Infringement of Copyright*, namely activities related to copyright.

In Article 14 of the European Treaty Series No. 185 (Convention 23.XI.2001), the scope of procedural provisions are given:

1. States parties should apply laws and other approaches necessary to establish the powers and procedures provided for in this section for the purpose of investigating specific criminal offences.
2. Unless as specifically stated otherwise in Article 21, States Parties shall apply the powers and procedures referred to in paragraph 1 of this Article to:
   a. criminal offences determined according to Articles 2 to 11.
   b. criminal acts committed through a computer system.
   c. collection of electronic evidence of a crime.

According to the Budapest Convention, its conclusions were published in the European Treaty Series Number 185 and is known as the Convention on Cybercrimes (Council of Europe, 2001b). After the Budapest convention, many countries began to ratify it to enable its implementation in their national law.

In accordance with the provisions of Article 36 paragraph (3) concerning the Signing and Enforcement of the Cybercrime Convention, the convention will enter into force 3 months after it has been ratified by five countries. Three of them must be member states of the Council of Europe. The convention was opened for signature on 23 November in Budapest, Hungary. Some of the countries that were expected to be the first signatories are Australia, Canada, New Zealand, Japan and the United States. Indeed, as earlier mentioned, this convention is not limited to only European countries but is open to all countries.

The role of Interpol in the process of requesting assistance without an agreement between countries in the event of a problem is contained in Article 27. In this case, there is no mutual agreement or statutory regulation in force between the requesting and requested parties. Each party must designate a central authority that would be responsible for sending and responding to requests for mutual assistance. Central authorities must communicate directly with each other. Thereafter, each party shall, at the time of signature or at the deposit of its instrument of ratification, acceptance, approval or accession, communicate with the Secretary-General of the Council of Europe the name and address of the authority designated.

Requests for mutual assistance must be carried out in accordance with the procedures prescribed by the requesting party, unless it is inconsistent with the laws of the requested party. In addition to the reasons for refusal set out in Article 25, the requested party may refuse the request if:

a. the request relates to a violation that the requested party deems to be a political infringement or an offense related to a political infringement, or
b. it considers that the implementation of the request may be contrary to its interests, security, public order or other interests.

The requested party may delay action upon request if such action would prejudice the criminal investigation or proceedings being carried out by its authorities. The requesting party may request that the requested party keep the facts of any request confidential, except to the extent necessary for execution. If the requested party is unable to comply with the request for confidentiality, the requested party must immediately inform the requesting party, which will then determine whether the request should be executed in any case.

In case of urgency, the request for mutual assistance or related communications may be sent directly by the judicial authority of the requesting party to such authority of the requested party. In such a case, a copy must be sent at the same time to the requested party's central authority through the requesting party's central authority. Any requests or communications based on the above pragraph may be made through the International Criminal Police Organization (Interpol).

In the event that an urgent request is submitted based on the process of submitting urgent request explained above, if the authority is not competent to handle the request, it shall refer the request to the competent national authority and inform directly the requesting party that it has done so. Each party may, at the time of signature or at the time of depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary-General of the Council of Europe that, for reasons of efficiency, request made under the above provisions shall be addressed to its central authority.

Relation Between Interpol with Non-States Party

Indonesia is not a party to the Budapest convention but almost all the types of cybercrimes contained in the Budapest convention have been adopted and regulated in the ITE Law No. 11 of 2008, Law on Copyright No. 44 of 2008, and Law on Child Pornography No. 28 of 2014. Cybercrime is regulated by the ITE Law especially in Articles 27 to 30, regarding prohibited acts.

In other hands, Indonesia is the member of international police organization (Interpol) whose major function is to ensure information exchange regarding transnational and international crimes between representatives of its member countries. Interpol (www.interpol.it) has created two secure and flexible

services to facilitate cybercrime-related communication among police and other stakeholders:

1. Cybercrime Knowledge Exchange workspace, which handles general, non-police information and is open to all relevant users. The workspace is open to law enforcement, governments, international organizations and cybersecurity industry experts to exchange non-police operational information on cybercrime.
2. Cybercrime Collaborative Platform-Operation, to support law enforcement operations, with access restricted to operational stakeholders only. The platform will enhance the operational efficiency and effectiveness of member countries. It will enable them to see the bigger picture of cyber threats and trends and therefore better focus their resources and avoid duplication of effort.

Interpol Indonesia is one of the bureaus within the organizational structure of the National Police International Relations Division (Divhubinter Polri); it is tasked with fostering, supervising and controlling the implementation of NCB-Interpol tasks for international cooperation in both bilateral and multilateral scopes.

Police cooperation, assistance and relations are regulated by the Law of the Republic of Indonesia Number 2 of 2002 and Government Regulation Number 17 of 2012 concerning the Police. Chapter VII, Article 41 of the Law of the Republic of Indonesia Number 2 of 2002 concerning the Police states as follows:

1) The state police of the Republic of Indonesia may request assistance from the Indonesian National Armed Forces in the context of carrying out security duties, which will be further regulated by a Government Regulation.
2) The police of the Republic of Indonesia can provide assistance to the Indonesian National Army in a state of military emergency and a state of war in accordance with the laws and regulations.
3) The state police of the Republic of Indonesia shall actively assist in the task of maintaining world peace under the banner of the United Nation (Sjamsudin, 2016: 22).

An example of a cybercrime case involving Interpol in Indonesia is the hacking case of the Surabaya Black Hat group in 2018. Polda Metro Jaya (a regional-level police in Indonesia) formed two teams to investigate the case. The police are working closely with FBI-Interpol to further investigate existing cases. It was determined that six actors hacked thousands of systems and websites, and a large amount of company and government agency data were compromised. Their activities were not limited to Indonesia, but they also hacked government systems abroad. About 42 countries were affected. They got thousands of US dollars from their illegal activities of extorting companies, and they damaged the websites of companies.

Conclusion

Based on the Budapest Convention held in Hungary in 2001, the performance of Interpol in the fight against cybercrime has greatly improved, since it stipulates specific procedures for the purpose of enhancing the investigation of specific crimes. Of course, Interpol is expected to act based on existing regulations, and the Budapest Convention has provided a detailed legal framework to enhance its activities regarding the eradication of cybercrime. Interpol have played an important role in solving cybercrime cases, given that the Budapest Convention has laid a solid legal foundation in the battle against cybercrime.***

References

Christien Pristi Gresilo Putri Amanda, Veriena Josepha Batseba Rehatta, Richard Marsilio Waas, Kedudukan *International Criminal Police Organization* (ICPO-Interpol) dalam Perjanjian Ekstradisi antara Indonesia dan Australia, TATOHI Jurnal Ilmu Hukum Vol 1, No 1 (2021).

Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.

Halder, D., & Jaishankar, K. (2011) Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

Constitution of International Criminal Police Organisation (Interpol).

Sjamsudin, Jen Rivaldi. *Kerjasama Interpol Dalam Penanganan International Crime Menurut Undangundang Kepolisian Nomor 2 Tahun 2002,* Lex Privatum, Vol. IV No. 7, (2016).

Budapest Convention on *Cybercrime* 2001.

Aisha Inayati, *Kerjasama Indonesia Dan Interpol Dalam Penanggulangan Illegal, Unreported* Dan *Unregulated Fishing,* Vol. 5 No. 3, (2019)

Ridwan Arifin, Hartini Atikasari, Waspiah, *The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud*, Jurnal Hukum Noelty, Vol. 11, Issue 02, (2020).

Widyawati, Anis. *Pengantar Hukum Pidana*. Jakarta: Sinar Grafika, 2014.

Rahardjo, Agus, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: Citra Aditya Bakti, 2002.

Suseno, Sigit, *Yurisdiksi Tindak Pidana Siber*, Bandung: Refika Aditama, 2012.

Wahid, Abdul dan Mohammad, Labib, *Kejahatan Mayantara: Cybercrime*, Bandung: Refika Aditama, 2005.