

**KERJASAMA INTERPOL DENGAN PEMERINTAH  
INDONESIA DALAM MENGHADAPI ANCAMAN  
CYBERCRIME PADA MASA PANDEMI COVID-19**

**SKRIPSI**

**Diajukan Untuk Memenuhi Sebagian Persyaratan Guna Menempuh  
Derajat Sarjana (S-1)  
Ilmu Hubungan Internasional**



**Disusun Oleh :**

**ANINDA NURAYGY HAJJISA**

**07041181924030**

**JURUSAN ILMU HUBUNGAN INTERNASIONAL**

**FAKULTAS ILMU SOSIAL DAN ILMU POLITIK**

**UNIVERSITAS SRIWIJAYA**

**2023**

HALAMAN PERSETUJUAN UJIAN SKRIPSI

**“Kerjasama INTERPOL dengan Pemerintah Indonesia dalam  
Menghadapi Ancaman Cybercrime pada Masa Pandemi COVID-19”**

**Disajikan untuk Memenuhi Sebagian Persyaratan dalam Menempuh**

**Derajat Sarjana S-1 Ilmu Hubungan Internasional**

Oleh :

**Aninda Nuraygy Hajjisa**

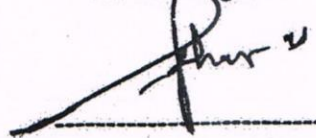
**07041181924030**

Pembimbing I

Dr. H. Azhar. SH., M.Sc.,LL.M

196504271989031003

Tanda Tangan



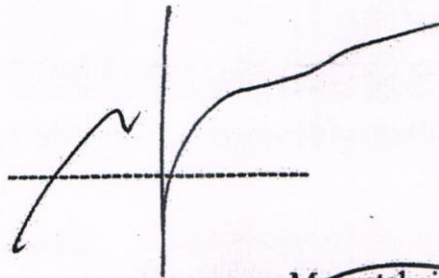
Tanggal

23 Februari 2023

Pembimbing II

Abdul Halim S.IP.,MA

199310082020121020



22 Februari 2023

Mengetahui,  
Ketua Jurusan,

Sofyan Effendi S.IP.,M.Si

NIP.1977851220031210003



HALAMAN PENGESAHAN UJIAN SKRIPSI

**“Kerjasama INTERPOL dengan Pemerintah Indonesia dalam Menghadapi  
Ancaman *Cybercrime* Pada Masa Pandemi COVID-19”**

Skripsi  
Oleh:  
**Aninda Nuraygy Hajjisa**  
**07041181924030**

**Telah dipertahankan di depan penguji  
Dan dinyatakan telah memenuhi syarat  
Pada tanggal 8 Maret 2023**

Pembimbing:

1. H. Azhar, SH., M.Sc., LL.M., LL.D  
NIP. 196504271989031003

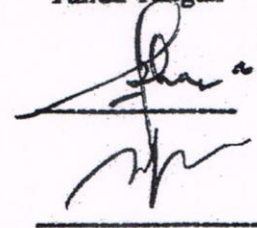
2. Abdul Halim, S.IP., MA  
NIP. 199310082020121020

Penguji:

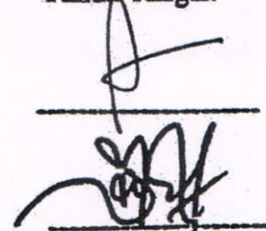
1. Nurul Aulia S.IP., MA  
NIP. 19931222202203201

2. Maudy Noor Fadhlia, S.Hub.Int., MA  
NIDN. 8948340022

Tanda Tangan



Tanda Tangan



Mengetahui,

Dekan FISIP UNSRI,

**Prof. Dr. Alftri, M.Si**  
**NIP. 196601221990031004**

Ketua Jurusan,

**Sofyan Effendi, S.IP., MSI**  
**NIP. 197705122003121003**

## LEMBAR PERNYATAAN ORISINALITAS

Saya yang bertanda tangan dibawah ini:

Nama : Aninda Nuraygy Hajjisa

NIM : 07041181924030

Jurusan : Ilmu Hubungan Internasional

Menyatakan dengan sungguh-sungguh bahwa skripsi yang berjudul “Kerjasama INTERPOL dengan Pemerintah Indonesia dalam Menghadapi Ancaman *Cybercrime* pada Masa Pandemi COVID-19” ini adalah benar-benar karya saya sendiri dan saya tidak melakukan penjiplakan atau pengutipan dengan cara yang tidak sesuai dengan etika keilmuan yang berlaku sesuai dengan Peraturan Menteri Pendidikan Nasional Republik Indonesia Nomor 17 Tahun 2010 tentang Pencegahan dan Penanggulangan Plagiat di Perguruan Tinggi. Apabila di kemudian hari, ada pelanggaran yang ditemukan dalam skripsi ini dan/atau ada pengaduan dari pihak lain terhadap keaslian karya ini, saya bersedia menanggung sanksi yang dijatuhkan kepada saya.

Demikian pernyataan ini dibuat dengan sungguh-sungguh tanpa pemaksaan dari pihak manapun.

Indralaya, 23 Februari 2023

Yang membuat pernyataan



Aninda Nuraygy Hajjisa

NIM. 07041181924030

## ABSTRAK

Pada masa Pandemi COVID-19 masyarakat harus membatasi aktivitas sehari-harinya yang biasa dilakukan tatap muka secara langsung dan harus diubah menjadi aktivitas yang dilakukan secara *online*. Meningkatnya aktivitas yang dilakukan secara *online* ternyata seiringan dengan meningkatnya kasus kejahatan siber yang terjadi di Indonesia. Indonesia dan kebanyakan negara-negara di kawasan Asia Tenggara masih memerlukan bantuan dari organisasi internasional untuk menghadapi ancaman siber yang kian terus meningkat. INTERPOL merupakan organisasi internasional yang memiliki perhatian khusus terhadap isu kejahatan siber di kawasan Asia Tenggara termasuk Indonesia dan memiliki proyek khusus terkait kejahatan siber di kawasan tersebut. Maka dari itu, penelitian ini dibuat untuk menganalisis bagaimana bentuk kerjasama yang dilakukan oleh INTERPOL dengan Pemerintah Indonesia dalam menghadapi ancaman *cybercrime* pada masa Pandemi COVID-19. Pada penelitian ini, untuk menganalisis bentuk kerjasama yang dilakukan, peneliti menggunakan konsep *Internal Police Cooperation* oleh Frederic Lemieux. Konsep *International Police Cooperation* akan digunakan untuk menganalisis bagaimana langkah-langkah terjadinya kerjasama antar polisi yang melewati lintas batas negara (transnasional). Penelitian ini menggunakan desain penelitian kualitatif deskriptif. Hasil yang didapatkan dari penelitian ini adalah terdapat beberapa jenis ancaman dengan kasus yang cukup tinggi dan akan dihadapi oleh Indonesia yaitu *Business Email Compromise (BEC)*, *Phishing*, *Ransomware*, dan *E-Commerce Data Interception*. Kemudian, dalam menjalankan kerjasama terdapat beberapa langkah penting yaitu pertukaran informasi melalui pusat data yang disebut dengan *Cybercrime Collaboration Services*, proyek bersama yang dilakukan untuk menghadapi ancaman *cybercrime*, kerangka kerjasama yang dirancang untuk melaksanakan operasi gabungan, dan langkah terakhir adalah pengembangan strategi melalui pembuatan panduan analisis ancaman serta panduan penyusunan strategi siber nasional. Keempat hal tersebutlah yang saling berhubungan dan menjadi bentuk kerjasama yang dilakukan oleh INTERPOL dengan Pemerintah Indonesia dalam menghadapi ancaman *cybercrime* selama masa pandemi COVID-19.

**Kata Kunci:** Covid-19, *Cybercrime*, Kerjasama, Indonesia, INTERPOL

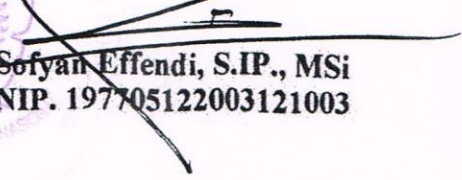
Pembimbing I

  
H. Azhar, SH., M.Sc., LL.M., LL.D  
NIP. 196504271989031003

Pembimbing II

  
Abdul Halim, S.IP., MA  
NIP. 199310082020121020

Mengetahui,  
Ketua Jurusan

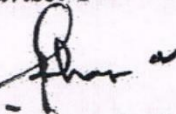
  
Sofyan Effendi, S.IP., MSi  
NIP. 197705122003121003

## ABSTRACT

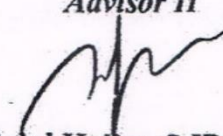
During the COVID-19 Pandemic, have to limit their daily activities that were usually carried out face-to-face and had to be changed to activities carried out online. The increase in activities carried out online is in line with the rise in cybercrime cases that have occurred in Indonesia. Indonesia and most countries in the Southeast Asian region still need assistance from international organizations to deal with the increasing cyber threats. INTERPOL is an international organization with particular attention to the issue of cybercrime in the Southeast Asian region, including Indonesia. It has special projects related to cybercrime in the region. Therefore, this research was made to analyze how the form of collaboration carried out by INTERPOL and the Government of Indonesia in dealing with cybercrime threats during the COVID-19 pandemic. In this study, to analyze the forms of cooperation carried out, researchers used the concept of International Police Cooperation by Frederic Lemieux. The concept of International Police Cooperation will be used to analyze the steps for cooperation between police that cross national borders (transnational). This study uses a descriptive qualitative research design. The results obtained from this study show that there are several types of threats with relatively high cases that Indonesia will face, namely Business Email Compromise (BEC), Phishing, Ransomware, and E-Commerce Data Interception. Then, in carrying out the collaboration, there are several necessary steps, namely the exchange of information through a data center called Cybercrime Collaboration Services; a joint project carried out to deal with cybercrime threats; a cooperation framework designed to carry out joint operations; and the last step is developing a strategy through making threats assessment as well as guidelines for drafting a national cyber strategy. These four interconnected things are a form of collaboration carried out by INTERPOL and the Government of Indonesia in dealing with cybercrime threats during the COVID-19 pandemic.

**Keywords:** Cooperation, COVID-19, Cybercrime, Indonesia, INTERPOL

Advisor I

  
H. Azhar, SH., M.Sc., LL.M., LL.D  
NIP. 196504271989031003

Advisor II

  
Abdul Halim, S.IP., MA  
NIP. 199310082020121020

Approved by,  
Head of Department

  
Sofyan Effendi, S.IP., MSi  
NIP. 197705122003121003



## KATA PENGANTAR

*Alhamdulillah Rabbil 'Alamin, segala puji dan syukur saya panjatkan kepada Allah SWT* atas rahmat serta karunia-Nya sehingga saya dapat menyelesaikan skripsi saya dengan tepat waktu. Skripsi ini dibuat sebagai salah satu dari syarat kelulusan dalam mencapai gelar Sarjana di bidang Ilmu Hubungan Internasional pada Fakultas Ilmu Sosial dan Ilmu Politik Universitas Sriwijaya. Saya sangat sadar bahwa penelitian ini berhasil diselesaikan karena banyaknya bantuan, bimbingan, dukungan, serta semangat yang diberikan oleh berbagai pihak dari awal perkuliahan hingga penyusunan skripsi ini. Maka dari itu, saya mengucapkan banyak terima kasih kepada:

1. Allah SWT. yang telah memberikan rahmat dan petunjuk-Nya sehingga saya dapat menjalani pendidikan dari awal perkuliahan hingga proses penyusunan skripsi ini dengan baik dan lancar.
2. Ibu (Meygy Carolin), Bapak (Bahrayen Sisten), dan Adik (Gen Raygy Siwanandau) yang selalu memberikan doa dan dukungan selama saya mengemban pendidikan.
3. Bapak Prof. Dr. Alfitri, M.Si. selaku Dekan dari Fakultas Ilmu Sosial dan Ilmu Politik Universitas Sriwijaya.
4. Bapak Sofyan Effendi, S.IP., M.Si. selaku Ketua Jurusan Ilmu Hubungan Internasional Universitas Sriwijaya.
5. Ibu Hoirun Nisyak, S.Pd., M.Pd. selaku Dosen Pembimbing Akademik selama perkuliahan saya di Universitas Sriwijaya.
6. Bapak H. Azhar, S.H., M.Sc., LL.M., LL.D dan Bapak Abdul Halim, S.IP., MA selaku Dosen Pembimbing Skripsi yang selalu memberikan bimbingan, arahan, dan bantuan kepada saya selama proses penyusunan skripsi.

7. Ibu Nurul Aulia, S.IP., MA dan Ibu Maudy Noor Fadhlia, S.Hub.Int, MA selaku Dosen Penguji Skripsi saya yang telah memberikan saran dan masukan untuk perbaikan skripsi saya.
8. Seluruh Civitas Akademika Fakultas Ilmu Sosial dan Ilmu Politik, khususnya dalam Jurusan Ilmu Hubungan Internasional.
9. Orang – orang baik yang saya temui selama masa perkuliahan, Bapak Halim yang menjadi orang tua kedua saya selama masa perkuliahan; Fatun, Mala, Yuk Nisa, Ubi, U One Gang, Four(bes), rekan – rekan di IRSSA, Aslab HI, dan HI C serta semua yang tidak dapat saya sebutkan satu persatu.
10. Terakhir, kepada diri saya sendiri. Terima kasih sudah bertahan sampai sejauh ini, terima kasih untuk tidak menyerah. Setelah ini akan ada tantangan yang jauh lebih besar lagi. Ayo terus berjuang lagi;

Saya sangat menyadari bahwa masih terdapat banyak kekurangan dan kesalahan dalam penelitian serta penulisan skripsi ini. Maka dari itu, saya mengucapkan permohonan maaf atas segala ketidaksempurnaan dari penelitian skripsi yang saya buat. Akhir kata, semoga skripsi ini dapat memberikan manfaat kepada saya sendiri dan juga pihak lainnya.

Indralaya, 22 Februari 2023



Aninda Nuraygy Hajjisa

NIM. 07041181924030



## DAFTAR ISI

<b>HALAMAN JUDUL .....</b>	<b>i</b>
<b>HALAMAN PERSETUJUAN UJIAN SKRIPSI .....</b>	<b>ii</b>
<b>HALAMAN PENGESAHAN UJIAN SKRIPSI .....</b>	<b>iii</b>
<b>LEMBAR PERNYATAAN ORISINALITAS .....</b>	<b>iv</b>
<b>ABSTRAK .....</b>	<b>v</b>
<b>ABSTRACT.....</b>	<b>vi</b>
<b>KATA PENGANTAR.....</b>	<b>vii</b>
<b>DAFTAR ISI.....</b>	<b>ix</b>
<b>DAFTAR TABEL .....</b>	<b>xi</b>
<b>DAFTAR GAMBAR.....</b>	<b>xii</b>
<b>DAFTAR SINGKATAN.....</b>	<b>xiii</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah.....	6
1.3 Tujuan Penelitian .....	6
1.4 Manfaat Penelitian .....	6
<b>BAB II TINJAUAN PUSTAKA .....</b>	<b>7</b>
2.1 Penelitian Terdahulu .....	7
2.2 Kerangka Teori .....	16
2.2.1 Kerjasama Internasional.....	16
2.2.2 <i>International Police Cooperation</i> .....	17
2.3 Alur Pemikiran.....	19
2.4 Argumentasi Utama .....	19
<b>BAB III METODE PENELITIAN .....</b>	<b>21</b>
3.1 Desain Penelitian .....	21
3.2 Definisi Konsep .....	21

3.3 Fokus Penelitian.....	24
3.4 Unit Analisis .....	25
3.5 Jenis dan Sumber Data.....	26
3.6 Teknik Pengumpulan Data.....	26
3.7 Teknik Keabsahan Data .....	27
3.8 Teknik Analisis Data .....	29
<b>BAB IV GAMBARAN UMUM PENELITIAN.....</b>	<b>30</b>
4.1 Jenis Ancaman <i>Cybercrime</i> di Indonesia.....	30
4.1.1 Kompromi Email Bisnis atau <i>Bussiness Email Compromise</i> (BEC).....	30
4.1.2 <i>Phishing</i> .....	32
4.1.3 <i>Ransomware</i> .....	34
4.1.2 <i>E-Commerce Data Interception</i> .....	36
4.2 Sejarah Kerjasama INTERPOL dan Pemerintah Indonesia.....	37
4.1.1 International Criminal Police Organization (ICPO) - INTERPOL.....	37
4.1.2 NCB INTERPOL Indonesia .....	40
<b>BAB V HASIL DAN PEMBAHASAN.....</b>	<b>44</b>
5.1 <i>Information Exchange</i> atau Pertukaran Informasi .....	44
5.2 <i>Organized Common Project</i> atau Proyek Bersama yang Terorganisir.....	46
5.3 <i>Working Groups</i> .....	59
5.4 <i>Strategy Development</i> atau Pengembangan Strategi.....	53
<b>BAB VI PENUTUP .....</b>	<b>60</b>
6.1 Kesimpulan .....	60
6.2 Saran .....	61
<b>DAFTAR PUSTAKA.....</b>	<b>62</b>
<b>LAMPIRAN.....</b>	<b>66</b>

## DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu .....	7
Tabel 2.2 <i>International Police Cooperation</i> .....	15
Tabel 3.1 Fokus Penelitian.....	24
Tabel 4.1 Kasus kejahatan phishing Januari – Juni 2020 .....	33

## DAFTAR GAMBAR

Gambar 1.1 Rata – rata Kasus Kejahatan Siber Perbulan di Indonesia .....	3
Gambar 2.1 Alur Pemikiran.....	19
Gambar 4.1 Grafik deteksi <i>ransomware</i> Januari – September 2020 .....	35
Gambar 4.2 Logo ICPO - INTERPOL .....	37
Gambar 4.3 Logo NCB INTERPOL Indonesia .....	41
Gambar 5.1 Kampanye <i>Good Cyber Hygiene</i> .....	48
Gambar 5.2 Perumusan Strategi Siber .....	55

## DAFTAR SINGKATAN

ACCDP	: <i>ASEAN Cyber Capacity Development Project</i>
ACTA	: <i>ASEAN Cyberthreat Assessment</i>
AJOC	: <i>ASEAN Joint Operations on Cybercrime</i>
ASEAN Desk	: <i>ASEAN Cybercrime Operations Desk</i>
BEC	: <i>Business Email Compromise</i>
C2	: <i>Command-and-Center</i>
CCP – Operation	: <i>Cybercrime Collaborative Platform – Operation</i>
CKE	: <i>Cybercrime Knowledge Exchange</i>
ICPC	: <i>International Criminal Police Commission</i>
ICPO	: <i>International Criminal Police Organization</i>
JAIF	: <i>Japan-ASEAN Integration Fund</i>
NCB	: <i>National Central Bureau</i>
UNODC	: <i>The United Nations Office on Drugs and Crime</i>
PSBB	: <i>Pembatasan Sosial Berskala Besar</i>
STP	: <i>Standard Tactical Plan</i>
WHO	: <i>World Health Organization</i>

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Istilah *cyberspace* atau “dunia maya” mulanya disampaikan oleh William Gibson pada tulisannya yang dibuat tahun 1982 dengan judul “Burning Chrome” untuk mendeskripsikan realitas virtual yang diciptakan oleh komputer. Namun, istilah tersebut menjadi populer pada tahun 1984, setelah digunakan dalam novel Gibson *Neuromancer*. Menurut Gibson, *cyberspace* adalah dunia nyata non-ruang, yang ditandai dengan kemampuan kehadiran virtual, serta adanya interaksi antara orang-orang melalui “ikon, titik arah, dan realitas buatan” (Kneale, 1999).

Keamanan siber merupakan isu yang sangat strategis dalam menjaga kestabilan suatu negara, khususnya di era modern ini. Ancaman yang dapat menyerang suatu negara tidak lagi berupa ancaman fisik atau tradisional tetapi juga ancaman siber. Perkembangan teknologi dan informasi yang begitu cepat, mampu membuat internet menjadi sebuah fenomena yang sangat berpengaruh dalam kehidupan sehari-hari. Kehadiran internet telah memberikan banyak kemudahan bagi setiap orang (Salsabilla, Fikri, Andika, & Harahap, 2020). Namun, pada perkembangannya ternyata penggunaan internet dalam segala aspek ini juga mempunyai bagian yang negatif. Internet mempengaruhi bentuk tindakan kejahatan, internet menyebabkan munculnya peluang terjadinya kejahatan yang selama ini tak pernah terpikirkan dan dianggap tidak mungkin terjadi. Kejahatan yang menjadi bagian negatif dari perkembangan internet inilah yang disebut sebagai kejahatan siber atau *cybercrime*. (Wardani, Warno, & Setiyono, 2016). Seiring teknologi digital menjadi semakin membludak ke dalam berbagai aspek pada kehidupan sehari-hari, dampak kejahatan dunia maya kian

meningkat. Kejahatan Siber yang terkait dengan pandemi COVID-19 pun turut kian meningkat. (INTERPOL, 2022).

Wabah mengejutkan yang dikenal sebagai virus corona (COVID-19) mengguncang dunia di penghujung tahun 2019, yakni pada sekitar bulan Desember. Wabah ini pada awalnya bermula atau muncul di kota Wuhan, China (Yuliana, 2020). Kemunculan wabah ini menjadi perhatian bagian seluruh masyarakat global, dan tepatnya pada akhir bulan Januari tahun 2020, WHO (World Health Organization) membuat pernyataan yang mengatakan bahwa COVID-19 telah menjadi suatu ancaman darurat bagi kesehatan di seluruh dunia (Dong et al., 2020).

Transmisi atau penyebaran COVID-19 antar negara terjadi cukup cepat dan hal ini seiring dengan peningkatan kasus yang terjadi di dunia. Indonesia menempati posisi keempat sebagai negara terpadat di dunia, kemudian negara Indonesia dikategorikan sebagai negara berkembang, sehingga diperkirakan Indonesia akan merasakan dampak yang cukup signifikan dan dalam jangka waktu yang lama akibat pandemi COVID-19 ini. Pemerintah Indonesia memberlakukan kebijakan *social distancing* serta menghimbau masyarakat dengan sosialisasi pedoman protokol kesehatan. Hal ini dilakukan pemerintah sebagai upaya menekan angka penyebaran kasus COVID-19 (Buana D.R., 2020).

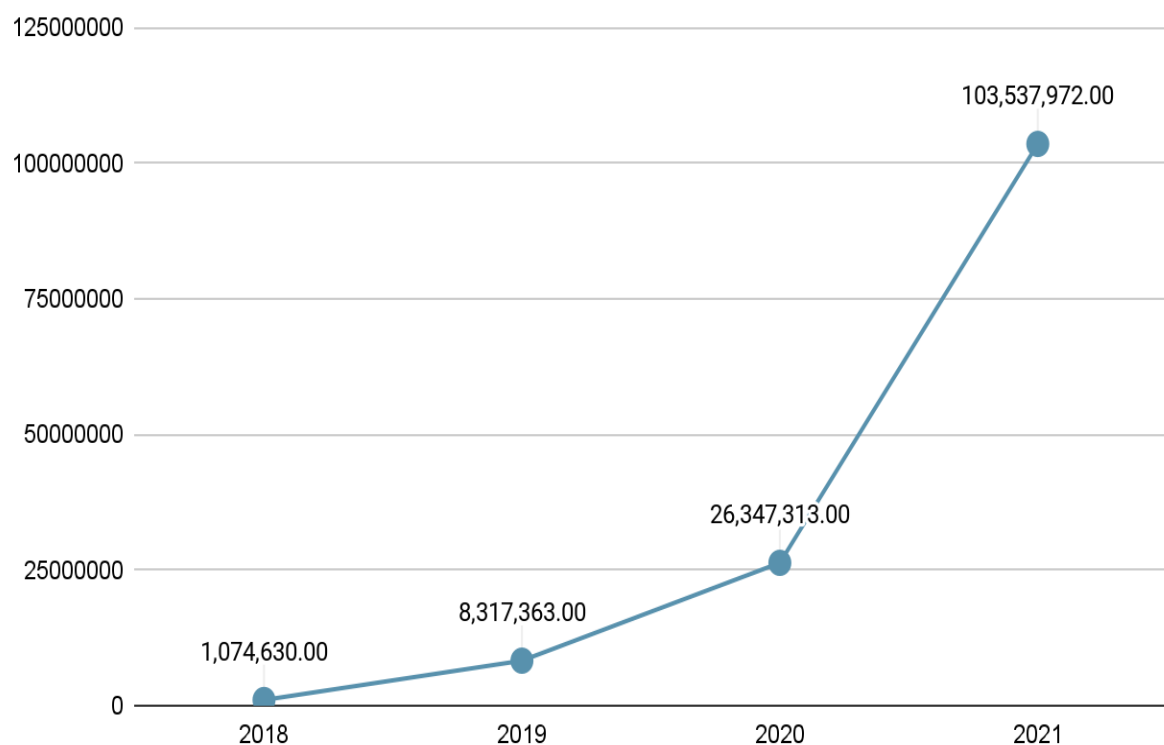
Tidak hanya itu, pemerintah juga menerapkan suatu kebijakan yang disebut sebagai Pembatasan Sosial Berskala Besar (PSBB). “Peraturan Pemerintah Nomor 21 Tahun 2020 tentang Pembatasan Sosial Berskala Besar dalam Rangka Percepatan Penanganan Corona Virus Disease 2019 (Covid-19)” memuat informasi mengenai kebijakan PSBB ini. Selama pemberlakuan kebijakan PSBB, ada beberapa hal yang dilarang, antara lain kegiatan kerja dan sekolah, kegiatan atau aktivitas keagamaan, kegiatan yang dilakukan secara langsung di ruang publik, serta penggunaan kendaraan umum. Sebagai dampak dari pemberlakuan kebijakan ini, maka sebagian besar kegiatan yang biasa dilakukan secara langsung dialihkan

kedalam kegiatan yang berbentuk online atau daring. Sehingga, selama masa pandemi COVID-19 terjadi, segala aktivitas yang dilakukan oleh masyarakat di dunia maya jauh meningkat.

Pada masa pandemi Covid-19, masyarakat perlu mewaspadaai banyaknya jenis kejahatan di dunia maya. Saat ini, ada semakin banyak jenis kejahatan dunia maya. Beberapa contoh kejahatan yang terjadi di dunia maya pada masa pandemi adalah orang yang meminta uang atas nama korban pandemi serta peretasan akun dan pencurian data.

**Gambar 1.1** Rata – rata kasus kejahatan siber perbulan di Indonesia

### Rata - rata kasus per-bulan



Sumber: HoneyNet Report



Berdasarkan grafik yang tertera, dapat dilihat bahwa pada tahun 2018, terjadi sebanyak rata-rata 1.074.630 serangan siber per bulan di Indonesia. Jumlah serangan siber setiap bulannya meningkat menjadi 8.317.363 pada tahun 2019. Kemudian, pada tahun 2020 meningkat lagi dan mencapai 26.347.313 per bulan. Selanjutnya, terdapat pula peningkatan yang sangat drastis pada tahun 2021, yaitu mencapai 103.537.972 serangan siber setiap bulan. Pada tahun 2020 kenaikannya masih tidak terlalu jauh karena masih bereaksi terhadap perubahan internet. Sementara itu, jumlah serangan siber per bulan meningkat cukup cepat pada tahun 2021, tahun dimana masyarakat sudah terbiasa menggunakan internet. Hal ini disebabkan oleh telah berlalunya masa transisi. Berdasarkan data ini, maka dapat dilihat bahwa pada masa pandemi COVID-19 ternyata terjadi peningkatan kejahatan siber yang sangat signifikan di Indonesia (Mulya et al., 2021).

Kasus kejahatan siber yang terjadi di dunia termasuk di Indonesia kian semakin meningkat seiring dengan berjalannya waktu. Para pelaku kejahatan siber terus mencari cela dan kesempatan untuk melancarkan aksi kejahatannya. Pemerintah dan Masyarakat Indonesia seharusnya lebih peduli dan sadar akan berbagai bentuk kejahatan siber yang dapat ditemui saat menggunakan internet (Chintia, et al., 2018). Menurut laporan INTERPOL “ASEAN Cyberthreat Assessment 2021”, bentuk- bentuk kejahatan siber atau *cybercrime* yang sangat mengancam Indonesia antara lain adalah *Business E-mail Compromise (BEC)*, *Phishing*, *Ransomware*, *E-Commerce data interception* (INTERPOL, 2021).

Negara-negara di kawasan Asia Tenggara termasuk Indonesia yang masih termasuk kategori “Dunia Ketiga” membutuhkan peran organisasi internasional untuk menjaga kedaulatannya. Dibandingkan dengan negara adidaya dan mayoritas negara Eropa, mayoritas negara-negara di kawasan Asia Tenggara masih lemah dalam menghadapi serangan siber. Serangan tersebut tidak mengakibatkan dampak yang terlihat, namun serangan tersebut secara bertahap dapat mengakibatkan kerusakan besar seperti konflik internal dan kerusakan

sistem (Salsabilla, Fikri, Andika, & Harahap, 2020). Peningkatan kasus yang terjadi di Indonesia ini menunjukkan bahwa pertahanan dan keamanan siber di Indonesia masih belum kuat sehingga membutuhkan bantuan berupa kerjasama dari organisasi internasional seperti INTERPOL dalam menghadapi kejahatan siber yang mengancam negara Indonesia.

Organisasi Internasional INTERPOL (International Criminal Police Organization) yang dibentuk dengan tujuan membantu polisi di seluruh negara harus melakukan perannya dengan baik dalam menghadapi ancaman *cybercrime* yang terjadi di seluruh negara, tak terkecuali Indonesia. INTERPOL sendiri merupakan organisasi internasional yang memiliki perhatian khusus akan ancaman *cybercrime* yang terdapat di kawasan Asia Tenggara. Perhatian ini ditunjukkan dengan diluncurkannya beberapa proyek inisiasi INTERPOL yang berfokus pada isu *cybercrime* di kawasan Asia Tenggara dan dimulai sejak tahun 2018 (INTERPOL, 2021).

INTERPOL berusaha untuk menjadi organisasi yang menginisiasi berjalannya kerjasama internasional dalam memerangi *cybercrime* melalui beberapa proyek. Penelitian ini akan menganalisis kerjasama yang dilakukan oleh INTERPOL dengan Pemerintah Indonesia dimana dalam hal ini yang dimaksud adalah NCB INTERPOL Indonesia. NCB INTERPOL Indonesia merupakan badan yang berdiri sebagai perwakilan pemerintah Indonesia dalam menjalin hubungan dengan NCB negara lain dan dengan Sekretaris Jenderal ICPO-INTERPOL. Oleh karena itu, dibuatlah penelitian yang berjudul “Kerjasama INTERPOL dengan Pemerintah Indonesia dalam Menghadapi Ancaman *Cybercrime* pada Masa Pandemi COVID-19”.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang penelitian yang telah diuraikan oleh peneliti sebelumnya, maka dari itu rumusan masalah pada penelitian ini adalah **“Bagaimana bentuk kerjasama INTERPOL dengan Pemerintah Indonesia dalam Menghadapi Ancaman *Cybercrime* pada Masa Pandemi COVID-19?”**

## **1.3 Tujuan Penelitian**

Berdasarkan rumusan masalah yang ada, maka penelitian ini dibuat dengan tujuan untuk menganalisis bagaimana bentuk kerjasama antara INTERPOL dengan pemerintah Indonesia dalam menghadapi ancaman – ancaman *cybercrime* yang terus meningkat di Indonesia pada masa pandemi COVID-19.

## **1.4 Manfaat Penelitian**

Penelitian yang berjudul “Kerjasama INTERPOL dengan Pemerintah Indonesia dalam Menghadapi Ancaman *Cybercrime* pada Masa Pandemi COVID-19” ini diharap dapat memberi manfaat antara lain:

### **a. Manfaat Teoritis**

Penelitian ini diharap dapat memberi manfaat dengan menjadi referensi literatur untuk melakukan penelitian selanjutnya yang terkait dengan topik serupa;

### **b. Manfaat Praktis**

Penelitian ini diharap dapat menjadi referensi bagi masyarakat untuk mengetahui bahaya yang mengancam keamanan individu di dunia maya atau dunia siber, serta bagaimana kerjasama internasional yang dilakukan oleh INTERPOL dengan Pemerintah Indonesia dalam menghadapi ancaman *cybercrime* pada masa pandemi COVID-19.

## DAFTAR PUSTAKA

- Agung, D. (2022). The Role of Interpol in the Settlement of Cybercrime Cases Under the Budapest Convention on Cybercrimes. *International Journal of Global Community Vol.5 No.1*, 49-56
- Azizah, R. (2016). PERANAN NCB-INTERPOL INDONESIA DALAM PROSES EKSTRADISI PELAKU KEJAHATAN TRANSNASIONAL (Studi Kasus: People Smuggling Sayed Abbas).
- Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks. *International Journal of Computer Applications Vol.182 No.33*, 27-29.
- Buana, D. R. (2020). Analisis Perilaku Masyarakat Indonesia dalam Menghadapi Pandemi Virus Corona (Covid-19) dan Kiat Menjaga Kesejahteraan Jiwa. National Research Tomsk State University, Universitas Mercu Buana.
- BSSN - IHP. (2019). *Laporan tahunan HoneyNet Project Tahun 2018*.
- BSSN - IHP. (2020). *Laporan tahunan HoneyNet Project Tahun 2019*.
- BSSN - IHP. (2021). *Laporan tahunan HoneyNet Project Tahun 2020*.
- BSSN - IHP. (2022). *Laporan tahunan HoneyNet Project Tahun 2021*.
- Chen, Q., & Bridges, R. A. (2017). Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. 16th IEEE International Conference on Machine Learning and Applications (ICMLA).
- Chintia, E., et al. (2018). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Educational Technology Vol.02 No.02*, 65-69.
- Connolly, L. Y., Wall, D. S., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity* , 1-18.
- Cybil. (2021). *National Cybercrime Strategy Guidebook*. Retrieved from Cybil Portal: <https://cybilportal.org/publications/national-cybercrime-strategy-guidebook/>
- Dougherty, J. E., & Pfaltzgraff, R. L. (1997). *Contending Theories of International Relation: A Comprehensive Survey* (4th Edition ed.). New York: Ed Addison Wesley Longman.
- Dong Y, Mo X, Hu Y, et al. (2020). Epidemiology of Covid-19 Among Children in China. *American Academy of Pediatrics*, DOI: 10.1542/peds.2020- 0702
- Faisal, S. (1992). *Format-format Penelitian Sosial*. Rajawali Press Jakarta

- Fourkas, V. (2004). What is 'cyberspace'? *Media Development*
- Goni, O., Ali, M. H., Showrov, Alam, M. M., & Shameem, M. A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, 29-39.
- Hamidi. (2010). Metode Penelitian Kualitatif Pendekatan Praktis Penulis Proposal dan Laporan Penelitian.. Malang : UU pers.
- Hasbiansyah, O. (2008). Pendekatan Fenomenologi: Pengantar Praktik Penelitian dalam Ilmu Sosial dan Komunikasi. *Mediator Vol. 9 No.1*, 163-180.
- HST. (2021, Juli 06). INTERPOL Offers National Cybercrime Strategy Guidebook. Retrieved from Homeland Security Today: <https://www.hstoday.us/subject-matter-areas/cybersecurity/interpol-offers-national-cybercrime-strategy-guidebook/>
- Inayati, A., & Windiani, R. (2019). KERJASAMA INDONESIA DAN INTERPOL DALAM PENANGGULANGAN ILLEGAL, UNREPORTED DAN UNREGULATED FISHING. *Journal of International Relations*, 5(3), 467-473  
<https://doi.org/10.14710/jirud.v5i3.24104>
- INTERPOL. (2022). ASEAN Cybercrime Operations Desk. Retrieved from INTERPOL: <http://www.interpol.int>
- INTERPOL. (2020). ASEAN Cyberthreat Assessment 2020
- INTERPOL. (2021). ASEAN Cyberthreat Assessment 2021
- INTERPOL. (2021). National Cybercrime Strategy Guidebook
- INTERPOL. (2023.). 1923 - how our history started. Retrieved from INTERPOL: <https://www.interpol.int/en/Who-we-are/INTERPOL-100/1923-how-our-history-started>
- ITU. (2021). *Global Cybersecurity Index* . Retrieved from International Telecommunication Union: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- Jackson, R., & Sorensen, G. (2013). *Introduction to International Relations: Theories and Approaches* (5th ed.). Oxford University Press.
- Kartasmita, K. (1997). Organisasi dan Administrasi Internasional. Bandung: Lembaga Penerbitan Sekolah Ilmu Administrasi
- Kaspersky. (2020). *Spam and Phishing Reports 2020*. Kaspersky.
- Kaspersky. (2022, Februari 09). Spam and Phishing in 2021. Retrieved from Securelist: <https://securelist.com/spam-and-phishing-in-2021/105713/>

- Lemieux, F. (2010). *International Police Cooperation: Emerging Issues, Theory and Practice*. Willan Publishing.
- Mekarisce, A. A. (2020). Teknik Pemeriksaan Keabsahan Data pada Penelitian Kualitatif di Bidang Kesehatan Masyarakat. *Jurnal Ilmiah Kesehatan Masyarakat* Vol. 12 No. 3, 145-151.
- Milner, H. (1992). International Theories of Cooperation Among Nations: Strengths and Weaknesses. *World Politics*, 44(03), 466-496.
- Moleong, Lexy J. (2007). *Metodologi Penelitian Kualitatif*. Penerbit PT Remaja Rosdakarya Offset, Bandung.
- Moreno, J. V. (2017). WannaCry Ransomware Attacks Should Be a Wake-Up Call for Cybersecurity Diligence. Retrieved from The National Law Review: <https://www.natlawreview.com/article/wannacry-ransomware-attacks-should-be-wake-call-cybersecurity-diligence>
- Mulya, N. B., Natasya P., K. D., Wangi, A. L., Nugraha, A. A., & Rimadhani, T. D. (2021, November 13). Analisis Peningkatan Jumlah Kasus *Cyber Attack* di Indonesia pada Masa Pandemi COVID-19. *Prosiding Seminar SITASI*.
- Murray, A. (2007). *The Regulation of Cyberspace, Control in the Online Environment*. Routledge.
- NCB-INTERPOL Indonesia. (n.d.). Profil NCB-Interpol Indonesia. Retrieved from NCB Interpol Indonesia: <https://interpol.go.id/profil.php>
- R., B. W. (2015). Peran INTERPOL dalam Memberantas Sindikat Cybersex di Filipina 2012 - 2014. *Journal of International Relations* Vol. 1 No.3, 25-29.
- Ramadhan, Iqbal. (2020). Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN). *Journal of Social and Political Sciences*. 3. 983-995. 10.31014/aior.1991.03.04.230.
- Sahir, S. H. (2021). *Metodologi Penelitian*. Bantul: PENERBIT KBM INDONESIA.
- Saksono, A. R. (2016). Fungsi dan Peran International Criminal Police Organization-INTERPOL dalam Ekstradisi. *Jurnal Kertha Negara* Vol. 04 No. 01, 1-5.
- Salsabilla, A. S., Fikri, M. D., Andika, M. S., & Harahap, N. A. (2020). Potential and Threat Analysis Towards Cybersecurity in South East Asia. *Journal of ASEAN Dynamics and Beyond* 1 (1), 1-12.
- Sari, A. K., Rahayu, S., Harjanti, W., Choifin, M., & Wahjoedi, T. (2021). *Metodologi Penelitian*. Surabaya: Penerbit Mengubah Semesta.

- Singh, A. C., Somase, K. P., & Tambre, K. G. (2013). Phishing: A Computer Security Threat Vol.1, No.7. *International Journal of Advance Research in Computer Science and Management Studies*, 64-71.
- Sugiyono. (2010). *Metode Penelitian Kuantitatif Kualitatif dan R&D*. Alfabeta Bandung.
- Tampubolon, K. E. (2019). Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare. *Jurisr-Diction Vol.2 No.2*, 539-554.
- UNODC. (2019). *Module 5: Cybercrime Investigation*. Retrieved from United Nations Office on Drugs and Crime: <https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html>
- Wall, D. S. (2005). The Internet as a Conduit for Criminal Activity. *Information Technology and the Criminal Justice System*, 77-98.
- Wardani, L. A., Warno, N. D., & Setiyono, J. (2016). Peran National Central Bureau (NCB) INTERPOL Indonesia dalam Pemberantasan Tindak Kejahatan Cybercrime. *Diponegoro Law Review*, 1-22.
- Warsino. (2020). Efek Pandemi Covid-19 terhadap Kejahatan Siber di Indonesia. *Tekinfor Jurnal Ilmiah Teknik Industri dan Informasi Vol.9 No.1 Hal.27-33*, Hal.27-33.
- WEF. (2021). The Global Risk Report 2021. World Economic Forum.
- Wiratama, O., Sutiarnoto, & Leviza, J. (2013). Peran Kerjasama Antara INTERPOL Indonesia dengan Malaysia Ditinjau dari Perspektif Hukum Internasional. *Journal of International Law Vol.01 No.1*, 1-15.
- World Bank. (2016). *Cybercrime Assessment Tool*. Retrieved from Combatting Cybercrime: <https://www.combattingcybercrime.org/#assessment>
- Yang, S. J., Holsopple, J., & Sudit, M. (2006). Evaluating Threat Assessment for Multi-Stage Cyber Attacks. *MILCOM*, 1-7.
- Yuliana. (2020). Corona Virus Disease (Covid-19); Sebuah Tinjauan Literatur. *Wellness and Healthy Magazine*, 2(1), 187-192.