SKRIPSI

TINJAUAN HUKUM PIDANA INTERNASIONAL TERHADAP SERANGAN SIBER MENGGUNAKAN VIRUS *RANSOMWARE WANNACRY* DI INDONESIA

OLEH:
ANDI RIAN JUBHARI
B11115375

DEPARTEMEN HUKUM INTERNASIONAL
FAKULTAS HUKUM
UNIVERSITAS HASANUDDIN
MAKASSAR
2021

HALAMAN JUDUL

TINJAUAN HUKUM PIDANA INTERNASIONAL TERHADAP SERANGAN SIBER MENGGUNAKAN VIRUS *RANSOMWARE WANNACRY* INDONESIA

OLEH

ANDI RIAN JUBHARI

B11115375

SKRIPSI

Sebagai Tugas Akhir dalam Rangka Penyelesaian Studi Sarjana pada

Departemen Hukum Internasional Program Studi Ilmu Hukum

DEPARTEMEN HUKUM INTERNASIONAL

FAKULTAS HUKUM

UNIVERSITAS HASANUDDIN

MAKASSAR

2021

LEMBAR PENGESAHAN SKRIPSI

TINJAUAN HUKUM PIDANA INTERNASIONAL TERHADAP SERANGAN SIBER MENGGUNAKAN VIRUS RANSOMWARE WANNACRY DI INDONESIA

Disusun dan diajukan oleh

ANDI RIAN JUBHARI
B11115375

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Departemen Hukum Internasional Program Studi Ilmu Hukum
Fakultas Hukum Universitas Hasanuddin
Pada tanggal 28 Desember 2021
Dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
Prof. Dr. Judhariksawan, S.H.,M.H.	Dr. Maskun, S.H.,LL.M.
NIP. 19690729 199903 1 002	NIP. 19761129 199903 1 005

Ketua Program Studi Sarjana Ilmu Hukum

Dr. Maskun, S.H., LL.M.
NIP. 19761129 199903 1 005

PERSETUJUAN PEMBIMBING

Diterangkan bahwa skripsi mahasiswa:

Nama	: Andi Rian Jubhari
NIM	: B11115375
Departemen	: Hukum Internasional
Judul	: Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus *Ransomware Wannacry* di Indonesia

Telah diperiksa dan disetujui untuk diajukan pada ujian skripsi.

Makassar, November 2021

Pembimbing Utama	Pembimbing Pendamping
Prof. Dr. Judhariksawan, S.H., M.H.	Dr. Maskun, S.H., LL.M.
NIP. 19690729 199903 1 002	NIP. 19761129 199903 1 005

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS HUKUM
Jln. Perintis Kemerdekaan KM.10 Kota Makassar 90245, Propinsi Sulawesi Selatan
Telp : (0411) 587219,546686, Website: https://lawfaculty.unhas.ac.id

PERSETUJUAN MENEMPUH UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama	: ANDI RIAN JUBHARI
N I M	: B11115375
Program Studi	: Ilmu Hukum
Departemen	: Hukum Internasional
Judul Skripsi	: Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus Ransomware WannaCry di Indonesia

Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir program studi.

Makassar, Desember 2021

an. Dekan
Wakil Dekan Bidang Akademik, Riset
dan Inovasi

Prof. Hamzah Halim, SH.,MH.,MAP
NIP. 19731231 199903 1 003

#generated_by_law_information_system_fh-uh in 2021-12-23 10:49:09

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini:

Nama	:	Andi Rian Jubhari
NIM	:	B11115375
Program Studi	:	Ilmu Hukum
Jenjang	:	S1

Menyatakan dengan ini bahwa Skripsi dengan judul Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus *Ransomware WannaCry* di Indonesia adalah karya saya sendiri dan tidak melanggar hak cipta pihak lain. Apabila di kemudian hari Skripsi karya saya ini terbukti bahwa sebagian atau keseluruhannya adalah hasil karya orang lain yang saya pergunakan dengan melanggar hak cipta lain, maka saya bersedia menerima sanksi.

Makassar, 28 Desember 2021

Andi Rian Jubhari

ABSTRAK

ANDI RIAN JUBHARI (B11115375), dengan judul "Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus *Ransomware WannaCry* di Indonesia." Dibawah bimbingan Judhariksawan sebagai Pembimbing Utama dan Maskun sebagai Pembimbing Pendamping.

Penelitian ini bertujuan untuk mengetahui bagaimana pengaturan mengenai serangan siber menggunakan virus *Ransomware WannaCry* dalam hukum pidana internasional. Serta untuk mengetahui bagaimana penindakan hukum terhadap serangan siber menggunakan virus *Ransomware WannaCry* di Indonesia.

Metode penelitian yang digunakan, yaitu normatif. Metode pengumpulan bahan hukum secara studi kepustakaan (*library research*). Bahan yang diperoleh berupa bahan hukum primer, bahan hukum sekunder (hasil-hasil penelitian, pendapat pakar hukum, dan buku teks), dan bahan hukum tersier (kamus hukum dan ensiklopedia) yang dianalisis secara sistematis, faktual, dan akurat.

Hasil penelitian ini menunjukkan bahwa (1) Kejahatan siber menggunakan virus *Ransomware WannacCry* diatur dalam *Convention on Cybercrime* 2001 dan pedoman-pedoman organisasi internasional sebagai kejahatan internasional. Walaupun demikian, penindakannya dibutuhkan kerjasama antar negara-negara mengingat virus ini terjadi lintas negara dan setiap negara memiliki kedaulatan dan sistem hukum yang harus dihormati oleh negara lainnya (2) Sistem hukum Indonesia sudah mengakomodir kriminalisasi untuk kejahatan siber menggunakan virus *Ransomware WannacCry* melalui KUHP, UU Telekomunikasi, dan UU ITE, tetapi untuk penindakan hukum terhadap serangan siber menggunakan virus *Ransomware WannaCry* di Indonesia masih sangat terbatas, karena penyelesaian kasus tersebut dilakukan secara mandiri oleh korban dengan membayar uang tebusan kepada pelaku atau merelakan datanya diambil oleh *hacker*.

Kata Kunci: Hukum Pidana Internasional; Serangan Siber; Virus *Ransomware Wannacry.*

ABSTRACT

ANDI RIAN JUBHARI (B11115375), with thesis title "International Criminal Law Review About Cyber Attack Using The WannaCry Ransomware Virus in Indonesia." Under guidance of Judhariksawan as Main Advisor and Maskun as Companion Advisor

This research aims to find out about the regulation regarding cyber attack using the WannaCry Ransomware virus in international criminal law. Also in order to find out about legal action againts cyber attack using the WannaCry Ransomware virus in Indonesia.

This research is a normative research where the sources are processed using interpretation methods. The legal materials used consist of primary legal materials, namely conventions, as well as secondary legal materials obtained from books, journals, and other related documents.

As for the result of this research, it's shown that (1) Cybercrime using the WannaCry Ransomware virus is regulated in the 2001 Convention on Cybercrime and international organization guidelines as an international crime. However, it's legal action requires cooperation between countries considering this virus occurs across countries and every country has sovereignity and legal system that must be respected by other countries. (2) The Indonesians law system has accommodated the criminalization of cybercrimes using the WannaCry Ransomware virus through the Criminal Code, the Telecommunications Law, and the Information and Electronic Transaction Law, but legal action againts cyber attacks using the WannaCry Ransomware virus in Indonesia is still very limited, because of the resolution of the case is carried out independently by the victim by pay a ransom to the hackers or let their data be taken by hackers.

Kata Kunci: International Criminal Law; Cyber Attack; WannaCry Ransomware Virus.

KATA PENGANTAR

Puji syukur Penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan karunia yang tak terhingga, sehingga Penulis dapat menyelesaikan skripsi dengan judul **"Tinjauan Hukum Pidana Internasional Terhadap Serangan Siber Menggunakan Virus *Ransomware WannaCry*"**. Penulis menyadari banyaknya kekurangan dalam penyusunan skripsi disebabkan keterbatasan dari Penulis.

Pada kesempatan ini, penulis ingin mengucapkan terima kasih sebesar-besarnya kepada kedua orang tua Penulis, H. Andi Mustari, S.H., M.Hum. dan Hj. Andi Matara Ariyanti yang telah membesarkan, merawat dan menyayangi Penulis dengan penuh kasih sayang serta memberikan didikan dan segalanya yang membangun pribadi Penulis menjadi lebih baik. Penyelesaian skripsi ini juga tidak terlepas dari adanya dukungan dan doa dari kakak-kakak Penulis, Andi Anugrah Pawalenrengi, S.H., M.H. dan drg. Andi Merlyana Mustari.

Seluruh kegiatan penyusunan skripsi ini tentunya tidak akan berjalan lancar tanpa adanya bantuan dan kerjasama dari berbagai pihak yang membantu kepada Penulis dalam penyusunan skripsi ini:

1. Terima kasih kepada Prof. Dr. Dwia Aries Tina Pulubuhu, MA. selaku Rektor Universitas Hasanuddin.
2. Terima kasih kepada Prof. Dr. Farida Pattitingi, S.H., M.Hum selaku Dekan Fakultas Hukum Unhas, beserta para Wakil

Dekan Prof.Dr. Hamzah Halim, S.H., M.H., Dr. Syamsuddin Muchtar, S.H., M.H., Dr. Muh. Hasrul, S.H., M.H., atas berbagai bantuan yang diberikan kepada Penulis, baik bantuan untuk menunjang berbagai kegiatan individual maupun yang dilaksanakan oleh Penulis bersama organisasi lain di Fakultas Hukum Universitas Hasanuddin.

3. Terima kasih kepada Prof. Dr. Judhariksawan, S.H., M.H. selaku Pembimbing Utama dan Dr. Maskun, S.H., LL.M. selaku Pembimbing Pendamping yang sudah sangat membimbing, membantu, mengarahkan serta memberikan saran yang sangat membangun dan bermanfaat kepada Penulis dalam penyelesaian skripsi ini. Penulis merasa sangat beruntung dapat dibimbing oleh kedua dosen yang sangat luar biasa.
4. Terima kasih kepada Prof. Dr. Juajir Sumardi, S.H., M.H., dan Dr. Laode Abd. Gani, S.H., M.H. selaku Dewan Penguji yang telah memberikan bimbingan, nasehat serta masukan kepada Penulis sehingga skripsi ini dapat terselesaikan.
5. Terima kasih kepada Ketua Bagian Hukum Internasional Dr. IIn Karita Sakharina, S.H., M.A., dan Sekretaris Bagian Hukum Internasional Dr. Laode Abd. Gani, S.H., M.H.
6. Terima kasih kepada Dr. Laode Abd. Gani, S.H., M.H. selaku Pembimbing Akademik Penulis yang telah memberikan bimbingan serta telah bersedia meluangkan waktu bagi Penulis

untuk konsultasi selama pengisian Kartu Rencana Studi (KRS) selama masa perkuliahan.

7. Terima kasih kepada segenap dosen Fakultas Hukum Universitas Hasanuddin yang telah memberikan ilmu pengetahuan dan pembelajaran kepada Penulis.
8. Seluruh staf/pegawai akademik yang senantiasa dengan sabar membantu penulis selama melakukan pemberkasan dan kebutuhan-kebutuhan penulis dalam penyelesaian skripsi ini.
9. Terima kasih kepada teman-teman MKU-F, yaitu Ahwal, Akbar, Aldri, Amel, Andini, Anna, Arum, Asel, Azza, Caca, Dejeng, Ocang, Fadel, Galuh, Hakim, Halima, Indra, Indri, Kevin, Kiky, Lian, Lisa, Mimi, Mufti, Uga, Rafi, Rahan, Hep, Rusdi, Sarput, Selvi, Sukardi, Yadin, Yogi, Yunda, Yusuf, Arman, dan Indah, yang telah menemani Penulis selama kehidupan perkuliahan, semoga pertemanan kita tetap terjaga selamanya.
10. Terima kasih kepada teman-teman Pengurus UKM Karate-do Gojukai Indonesia Fakultas Hukum Universitas Hasanuddin Andim, Fajar, Khaerul, Rifki, Ira, Aul, Lely, Awi, Yanuar, Niswar, Hafid, Aat, Kak Ocha, Kak Fel, Kak Winda, Kak Izzah, Kak Lisa, Kak Uga, Kak Akbar, Kak Jemmi, Kak Yudi dll. yang tidak dapat Penulis sebutkan satu-persatu, yang sudah memberikan pengalaman organisasi yang berharga bagi Penulis.

11. Terima kasih untuk teman-teman Pengurus Lembaga Penalaran dan Penulisan Karya Ilmiah Fakultas Hukum Universitas Hasanuddin Dyah, Kinkin, Jusi, Ari, Mufti, Renih, Lian, Hakim, Kak Refah, Kak Yusran, Kak Mirda, Kak Rani, Rizqa, Resty, Wardi, Asad, Adam, Akbar, Egy, Arham, Ririn, Ayu, dll. yang tidak dapat Penulis sebutkan satu-persatu, yang sudah banyak membantu Penulis keluar dari zona nyaman dan memberikan pengalaman organisasi yang berharga bagi Penulis.
12. Terima kasih untuk teman-teman International Law Students Association (ILSA) , yang sudah banyak membantu Penulis memberikan pengalaman organisasi yang berharga bagi Penulis.
13. Terima kasih untuk Executive Board International Law Students Association (ILSA) Universitas Hasanuddin kepengurusan 2017-2018, Kak Melly, Kak Vena, Kak Yati, Kak Angel , Andini, Aqiva, Ivon, Galuh, Trisna, Difa, Kak Kevin, Mimi,Octa, Eka, Hep dan Hans atas segala ilmu dan bantuan yang telah diberikan kepada Penulis serta kepercayaan yang diberikan kepada Penulis selaku Minister of Information and Technology. Juga kepada kakak-kakak yang selalu memberikan arahan dan banyak bantuan.
14. Terima kasih kepada teman-teman seperjuangan di Departemen Hukum Internasional, yaitu Wildan, Arum, Uga

Ahwal, Andini, Galuh, Trisna, Hep, Octa, Naya, Ivone, Lisa, Fikar, Imo, Hasbi, Halima, Arme, dan Clara, semoga pertemanan kita tetap terjaga selamanya.

15. Terima kasih kepada teman-teman JURIS 2015 atas segala bantuannya selama ini dan selamat berjuang untuk ke depannya.
16. Terima kasih kepada AKP Hariwibowo selaku Penyidik Direktorat Tindak Pidana Siber Bareskrim Polri, yang telah membantu Penulis sebagai narasumber dalam skripsi ini.
17. Terima kasih kepada bapak Supapri Situmorang, S.Tr.T., M.H. selaku Anggota Direktorat Keamanan Siber Badan Siber dan Sandi Negara, yang telah membantu Penulis sebagai narasumber dalam skripsi ini.
18. Terima kasih kepada bapak Samsaraji Bunayya dari Sekolah Hacker, yang telah membantu Penulis sebagai narasumber dalam skripsi ini.
19. Terima kasih kepada bapak Josua Sitompul, S.H., M.M. selaku pakar hukum siber, yang telag membantu Penulis sebagai narasumber dalam skripsi ini.
20. Terima kasih kepada Ibu Rosmalania, S.H., M.H. yang telah mendukung dan membantu Penulis selama proses pengerjaan skripsi ini.

21. Terima kasih kepada teman-teman KKN Reguler Gelombang 99 Desa Bonto Bunga Kecamatan Moncongloe, Vika, Fathin, Mirna, Ade, dan kak Ozan atas kerja samanya dalam menjalankan program kerja KKN dan telah menjadi teman posko terbaik serta memberikan pengalaman yang berharga bagi Penulis.

Skripsi ini masih jauh dari sempurna walaupun telah banyak menerima bantuan dari banyak pihak. Apabila terdapat kesalahan dalam skripsi ini, sepenuhnya menjadi tanggung jawab Penulis. Oleh karena itu, Penulis dengan segala kerendahan hati menerima setiap kritik dan saran yang membangun dari semua pihak, sehingga tugas akhir ini dapat bermanfaat bagi para pembaca

Makassar, Desember 2021

Andi RIan Jubhari

DAFTAR ISI

Halaman

HALAMAN JUDUL i

PENGESAHAN SKRIPSI ii

PERSETUJUAN PEMBIMBING ..... **Error! Bookmark not defined.**

PERSETUJUAN MENEMPUH UJIAN SKRIPSI iv

PERNYATAAN KEASLIAN v

ABSTRAK vi

ABSTRACT vii

KATA PENGANTAR viii

DAFTAR ISI xiv

BAB I PENDAHULUAN 1

A. Latar Belakang 1

B. Rumusan Masalah 7

C. Tujuan Penelitian 7

D. Kegunaan Penelitian 7

E. Keaslian Penelitian 8

F. Metode Penelitian 11

BAB II TINJAUAN PUSTAKA DAN ANALISIS PERMASALAHAN PERTAMA 15

A. Hukum Pidana Internasional 15

1. Hukum Definisi Hukum Pidana Internasional 15

2. Sumber Hukum Pidana Internasional 17

3. Karakteristik Tindak Pidana Internasional 20

B. Kejahatan Siber 23

C. Ransomware 40
1. Sejarah Virus *Ransomware* 40
2. Definisi Virus Ransomware 41
D. Analisis Pengaturan Mengenai Serangan Siber Menggunakan Virus *Ransomware Wannacry* Dalam Hukum Pidana Internasional 42
BAB III TINJAUAN PUSTAKA DAN ANALISIS PERMASALAHAN KEDUA 62
A. Kejahatan Siber Dalam Undang-Undang Informasi dan Transaksi Elektronik 62
1. Konten Ilegal 63
2. Akses Ilegal 65
3. Intersepsi Ilegal 66
4. Gangguan Terhadap Data 67
5. Gangguan Terhadap Sistem 67
6. Penyalahgunaan Perangkat 68
7. Pemalsuan yang Berhubungan Dengan Komputer 68
B. Analisis Penindakan Hukum Terhadap Serangan Siber Menggunakan Virus *Ransomware Wannacry* di Indonesia 69
BAB IV 78
PENUTUP 78
A. Kesimpulan 78
B. Saran 79
DAFTAR PUSTAKA 81
LAMPIRAN 87

BAB I

PENDAHULUAN

A. Latar Belakang

Secara alamiah, manusia tidak mungkin dilepaskan dari kemajuan teknologi yang tujuannya adalah untuk memudahkan kehidupannya. Secara alamiah pula, manusia tidak mungkin dilepaskan dari hukum yang tujuannya adalah untuk menjaga eksistensi.[1] Pada awalnya, manusia berkomunikasi dengan bertatap muka secara langsung dan saling memberikan isyarat tertentu, kemudian berkembang dengan menggunakan suatu perpaduan kata-kata tertentu yang bisa dipahami satu sama lain.

Sejarah mencatat bahwa manusia tradisional telah menggunakan lambang-lambang isyarat sebagai alat komunikasi. Sekitar lima ratus tahun sebelum Masehi, Darius, raja Persia menempatkan prajuritnya di setiap puncak bukit lalu mereka saling berteriak satu sama lain untuk menyampaikan informasi. Sementara itu bangsa Indian dapat berkomunikasi pada jarak puluhan mil dengan teknik hembusan asap. Bentuk tulisan yang pertama digunakan adalah piktograf dari orang Sumeria (3000 SM) yang sesungguhnya berupa gambar benda yang tampak sehari-hari. Kemudian piktograf berubah menjadi simbol-simbol yang dapat menggambarkan bunyi mulai muncul hingga pada akhirnya menjadi abjad modern. Penggunaan piktograf adalah titik awal komunikasi

[1] Edmon Makarim, 2004, *Kompilasi Hukum Telematika*, PT. Rajagrafindo Persada, Jakarta, hlm. 3.

tulisan yang berkembang semakin cepat dengan ditemukannya papirus[2] yang memungkinkan terjadinya komunikasi jarak jauh dengan media surat, baik yang diantar dengan menggunakan jasa pelari maraton, burung merpati, kuda maupun kereta api. Penemuan mesin cetak di China pada abad ke-10, yang disempurnakan oleh Johannes Guttenberg pada tahun 1440, kemudian mengantar manusia untuk mengenal media komunikasi massa cetak atau surat kabar pada abad ke-17.[3]

Seiring perkembangan manusia dari waktu ke waktu, kebutuhan manusia akan informasi dan komunikasi semakin mendorong manusia untuk mencoba menemukan dan mengembangkan media komunikasi baru yang mutakhir, yang memberikan kemungkinan kepada manusia untuk mengadakan komunikasi dan penyebaran informasi secara cepat dan tepat. Dengan berjalannya proses penemuan dan pengembangan media komunikasi dan informasi kemudian menghadirkan sebuah teknologi yang dapat memperlancar arus komunikasi dan informasi tanpa terhalang oleh ruang, batas, jarak, dan waktu, serta dapat meningkatkan produktifitas serta efisiensi, yang kemudian dikenal dengan teknologi informasi dan komunikasi (TIK).

Dalam era informasi (*information age*), keberadaan suatu informasi menjadi suatu hal yang sangat penting bagi orang yang akan mencari suatu informasi tertentu yang sesuai dengan kebutuhannya, dan tidak

[2] Papirus adalah alang-alang air yang digunakan sebagai bahan kertas tulis oleh orang zaman dahulu.

[3] Judhariksawan, 2005, *Pengantar Hukum Telekomunikasi*, Rajagrafindo Persada, Jakarta, hlm. 1-2.

kalah penting keakuratan data yang diperoleh menjadi suatu alasan untuk menggunakan teknologi informasi dan komunikasi (TIK). Dalam hal ini, TIK menjadi suatu media yang menjawab kebutuhan manusia akan pemenuhan suatu informasi dan komunikasi.

TIK telah membawa manusia kepada suatu peradaban baru dengan struktur sosial dan tata nilai yang diatur sedemikian rupa. Dalam perkembangannya, telah ditemukan komputer sebagai suatu produk yang lahir dari teknologi informasi dan komunikasi. Konvergensi antara teknologi telekomunikasi, media dan informatika menghadirkan suatu sarana baru yang disebut dengan internet.[4] Internet dapat diartikan sebagai jaringan komunikasi elektronik yang menghubungkan jaringan komputer dan fasilitas komputer yang terorganisasi di seluruh dunia melalui telepon atau satelit.[5]

Dengan internet manusia dapat melakukan aktivitas layaknya kehidupan di dunia nyata, manusia dapat melakukan berbagai hal dan berbagai aktivitas di dunia internet, mulai dari hanya sekedar mengobrol, transaksi bisnis secara *online*, berbelanja di toko *online*, dan lain sebagainya. Internet seakan telah membentuk suatu realitas baru yang menjadikannya menciptakan suatu dunia baru, dengan demikian secara tidak sengaja membagi kehidupan ini menjadi dua, yaitu kehidupan di dunia nyata (*real life)* dan kehidupan di dunia maya (*virtual life)*.

[4] Edmon Makarim, *Op.Cit*., hlm. 4.
[5] Kamus Besar Bahasa Indonesia.

Dengan demikian, bahwa dunia maya yang dibangun melalui jaringan internet dapat membangun dunia baru bagi para penggunanya yang dapat menimbulkan efek positif maupun negatif. Internet telah membangun sebuah dunia maya yang sebenarnya yaitu merupakan dunia tanpa batas serta dunia yang dapat dimasuki dan dimanfaatkan oleh siapa saja.

Perkembangan internet yang semakin pesat dan penggunanya yang semakin meningkat memungkinkan akan terjadinya suatu tindak pidana melalui dunia maya yang sering dikenal dengan nama *cybercrime* atau kejahatan siber. Kejahatan siber merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh bidang kehidupan modern saat ini.[6] Kejahatan siber menjadi sebuah fenomena baru dalam dunia kejahatan, karena kejahatan siber ini dapat dilakukan oleh seorang diri maupun beramai-ramai dan tidak mengenal batas negara (*borderless)*.

Salah satu kasus kejahatan siber yang pernah terjadi adalah serangan virus *Ransomware WannaCry*. Serangan ini terjadi pada tahun 2017 yang diperkirakan menginfeksi 300.000 sistem komputer di 150 negara.[7] Virus ini adalah sejenis *Ransomware* yang bernama *WannaCry* dimana virus ini menyandera *file* milik korbannya yang ada di dalam

[6] Barda Nawawi Arief, 2005, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*, Rajagrafindo Persada, Jakarta, hlm. 1.

[7] Oik Yusuf, *Kronologi Serangan Ransomware WannaCry yang Bikin Heboh Dunia*, diakses melalui https://tekno.kompas.com/read/2017/05/15/09095437/kronologi.serangan.ransomware.wannacry.yang.bikin.heboh.internet?page=all pada tanggal 23 Oktober 2019 pukul 07.51 Wita.

komputer dengan metode enkripsi[8] yang sulit ditembus. Bila korban ingin mendapatkan kunci enkripsi sehingga *file* yang disandera bisa diakses lagi, maka mereka harus membayar uang tebusan sejumlah $300 dalam bentuk *bitcoin* melalui tautan yang tertera di layar komputer korban ketika virus ini menginfeksi.

Virus *Ransomware WannaCry* ini awalnya adalah senjata siber milik *National Security Agency* (NSA) Amerika Serikat yang bernama *EternalBlue*. *EternalBlue* merupakan program anti teroris yang digunakan untuk mengambil data dari komputer sasaran NSA yang dianggap mengancam negara Amerika Serikat. Namun, pada tanggal 14 April 2017 program ini dicuri oleh kelompok *hacker* bernama *Shadow Broker* dan menghilang hingga akhirnya serangan *Ransomware WannaCry* ini terjadi.[9]

Serangan virus *Ransomware WannaCry* ini terdeteksi pertama kali pada tanggal 12 Mei 2017. Serangan ini menyerang komputer di seluruh dunia baik itu komputer milik perorangan, perusahaan, bahkan lembaga pemerintahan. Seperti di Eropa, pabrik mobil Nissan di Britania Raya terpaksa harus menghentikan produkisnya karena *ransomware WannaCry* menginfeksi beberapa sistem komputer mereka begitupun pabrik mobil Renault di Perancis. Sedangkan di Brazil, lembaga jaminan sosial milik pemerintah terpaksa harus memutuskan sambungan komputer dan menutup akses publik ke servernya untuk mencegah penyebaran virus

[8] Metode pengodean data agar komputer tidak dapat membaca atau menggunakan data.

[9] Anonim. *What is WannaCry ransomware?*. Diakses melalui https://www.kaspersky.com/resource-center/threats/ransomware-wannacry pada tanggal 29 Agustus 2019 pada pukul 16.23 Wita

ransomware wannacry ke komputer milik umum. Yang paling terdampak parah adalah lembaga pendanaan kesehatan Inggris (NHS) yang harus menunda setiap aliran pendanaan ke rumah sakit-rumah sakit yang ada di Inggris dikarenakan beberapa komputer mereka terinfeksi *ransomware wannacry* yang mengakibatkan 19.000 pasien di Inggris yang akan didanai penindakannya harus ditunda.[10]

Di Indonesia virus ini terdeteksi pada bulan Mei 2017 yang tidak hanya menyerang komputer pribadi tetapi juga korporasi, bahkan virus ini menyerang sistem komputer salah satu rumah sakit di Jakarta sehingga mengalami kelumpuhan dalam melayani pasien. Berdasarkan penelitian Avast Antivir, Avast telah memblok 54 juta serangan selama bulan Maret 2018 di seluruh dunia. Di Indonesia sendiri Avast telah berhasil memblok 17 juta lebih serangan *WannaCry* terhitung selama periode dari tanggal 5 Desember 2017 sampai 4 Januari 2018.[11]

Dalam masyarakat internasional aturan hukum mengenai kejahatan siber diatur dalam *Council of Europe Convention on Cybercrime* (ETS No. 185) di Budapest atau yang dikenal dengan *Budapest Convention on Cybercrime*, 2001. Sedangkan dalam hukum nasional, kejahatan siber atau tindak pidana siber telah diatur dalam Undang-Undang Nomor 19

[10] Roger Collier, *NHS Attack Spreads Worldwide*, diakses melalui https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5461132/ pada tanggal 23 Oktober 2019 pukul 09.02 Wita.

[11] Muhammad Alif Goenawan, *Serangan WannaCry di Indonesia Terbesar Kedua di Dunia*, diakses melalui https://inet.detik.com/security/d-4007294/serangan-wannacry-di-indonesia-terbesar-kedua-di-dunia pada tanggal 23 Oktober 2019 pukul 09.14 Wita.

Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

B. Rumusan Masalah

1. Bagaimana pengaturan mengenai serangan siber menggunakan virus *Ransomware WannaCry* dalam hukum pidana internasional?
2. Bagaimana penindakan hukum terhadap serangan siber menggunakan virus *Ransomware WannaCry* di Indonesia?

C. Tujuan Penelitian

1. Untuk mengetahui bagaimana pengaturan mengenai serangan siber menggunakan virus *Ransomware WannaCry* dalam hukum pidana internasional.
2. Untuk mengetahui bagaimana penindakan hukum terhadap serangan siber menggunakan virus *Ransomware WannaCry* di Indonesia.

D. Kegunaan Penelitian

Penelitian ini diharapkan dapat memberikan kegunaan atau manfaat secara teoritis dan praktis, yaitu sebagai berikut:

1. Kegunaan Teoritis

Kegunaan teoritis penelitian ini diharapkan dapat menambah acuan bagi pengembangan penelitian terkait hukum internasional, khususnya terkait kejahatan siber.

2. Kegunaan Praktis

   Kegunaan praktis penelitian ini diharapkan dapat memberikan wawasan dan pengetahuan khususnya penulis dan umumnya bagi para mahasiswa hukum mengenai kejahatan siber, serta sebagai literatur tambahan bagi yang berminat untuk meneliti lebih lanjut tentang kejahatan siber.

E. Keaslian Penelitian

Berdasarkan analisis Penulis untuk memberikan gambaran komparasi untuk menyatakan keaslian skripsi, Penulis melampirkan 3 skripsi sebagai bahan perbandingan terhadap tulisan ini,yaitu:

1. Skripsi atas nama Sukma Indrajati, Fakultas Hukum Universitas Hasanuddin tahun 2014. Penelitian Sdri. Sukma berjudul “Tinjauan Hukum Internasional Terhadap *Cyber Espionage* Sebagai Salah Satu Bentuk *Cybercrime*”. Penelitian Sdri. Sukma merupakan penelitian yuridis-normatif yaitu penelitian terhadap asas-asas hukum, aturan-aturan hukum yang ada untuk mendapatkan informas tentang *cyber espionage*. Metode pengumpulan bahan hukum yang dilakukan oleh Sdri. Sukma melalui studi lapangan serta studi kepustakaan. Fokus utama permasalahan dari penelitian Sdri. Sukma ialah apakah hukum

internasional mengatur mengenai *cyber espionage* serta bagaimana bentuk perlindungan yang diberikan terhadap serangan *cyber espionage* di Indonesia. Penelitian Sdri. Sukma menyimpulkan bahwa instrument hukum internasional mengenai kejahatan siber terutama yang menyangkut mengenai *cyber espionage* pada umumnya merupakan instrument regional. Salah satu contohnya adalah *Convention on Cybercrime* yang dibuat oleh *Council of Europe*, sehingga diperlukan adanya instrument hukum mengenai kejahatan siber skala internasional walaupun sebelumnya telah ada beberapa upaya mengenai hal tersebut seperti dalam Kongres ke-12 tentang Pencegahan Kejahatan dan Peradilan Pidana di Brazil.[12]

2. Skripsi atas nama Haryo Andi Setiaji, Fakultas Hukum Universitas Hasanuddin 2016. Penelitian Sdr. Haryo berjudul *"*Tinjauan Hukum Internasional Terhadap Kasus *Hackin*g Sony Pictures Enterainment". Penelitian yang dilakukan Sdr. Haryo menggunakan metode *"library research"* atau studi kepustakaan. Sdr. Haryo melakukan pengumpulan data-data yang diperoleh dari buku-buku, hasil penelitian, jurnal ilmiah, dan bahan-bahan tertulis lainnya serta pencarian informasi melalui internet yang berhubungan dengan kasus *hacking* Sony Pictures Entertainment. Hasil dari penelitian Sdr. Haryo menunjukkan bahwa dalam kasus *hacking* Sony Pictures Entertainment terdapat berbagai bentuk kejahatan siber seperti *illegal*

[12] Sukma Indrajati, 2014, *"Tinjauan Hukum Internasional Terhadap Cyber Espionage Sebagai Salah Satu Bentuk Cybercrime"*, Skripsi, Sarjana Hukum, Fakultas Hukum Universitas Hasanuddin, Makassar.

access, system interference, infringement of copyright and related rights, dan *infringement of privacy* yang dimana kejahatan-kejahatan tersebut telah diatur dalam regulasi internasional dan juga kasus *hacking* Sony Pictures Entertainment merupakan kejahatan transnasional.[13]

3. Skripsi atas nama Oktaviani Sugiarto , Fakultas Hukum Universitas Hasanuddin 2019. Penelitian Sdri. Okta berjudul "Tinjauan Hukum Internasional Terkait Perlindungan Data dan Informasi Pribadi". Penelitian yang dilakukan Sdri. Okta menggunakan metode *"library research"* atau studi kepustakaan. Sdri. Okta melakukan pengumpulan data-data yang diperoleh dari buku-buku, hasil penelitian, jurnal ilmiah, dan bahan-bahan tertulis lainnya serta pencarian informasi melalui internet yang berhubungan dengan data privasi. Adapun hasil penelitian dari Sdri. Okta menyimpulkan (1) pelanggaran terhadap data privasi merupakan kejahatan transnasional yang berkaitan dengan tindak pidana kejahatan siber. Meskipun belum ada perjanjian internasional yang mengikat secara global mengenai perlindungan data privasi, akan tetapi terdapat peraturan dan konvensi yang telah disepakati dan diadopsi oleh negara-negara, yang di dalamnya terdapat prinsip-prinsip yang dapat digunakan untuk melindungi data pribadi subjek data atau digunakan sebagai dasar hukum dalam pemidanaan pelanggaran terhadap data

[13] Haryo Andi Setiaji, 2016, *"Tinjauan Hukum Internasional Terhadap Kasus Hacking Sony Pictures Entertainment"*, Skripsi, Sarjana Hukum, Fakultas Hukum Universitas Hasanuddin, Makassar.

privasi. (2) hak atas privasi tidak bertentangan dengan hak asasi manusia melainkan merupakan bagian dari HAM yang fundamental (tidak mutlak) . Namun, dalam penerapannya hak privasi dapat dibatasi/dilanggar secara sah oleh undang-undang.[14]

Berdasarkan pemaparan tiga bahan perbandingan di atas. Penulis dalam penelitian ini mencoba untuk menjelaskan bagaimana pengaturan mengenai serangan siber menggunakan virus *Ransomware WannaCry* dalam hukum pidana internasional dan bagaimana penindakan hukum terhadap serangan siber menggunakan virus *Ransomware WannaCry* di Indonesia. Dapat dilihat dari objek penelitian hingga fokus kajian yang akan diteliti oleh Penulis merupakan sebuah kebaruan.

F. Metode Penelitian

Adapun metode penelitian yang digunakan oleh Penulis dalam penelitian ini adalah sebagai berikut:

1. Jenis Penelitian

Jenis penelitian ini merupakan penelitian hukum normatif-empiris, yaitu metode penelitian yang dalam hal ini menggabungkan unsur hukum normatif yang kemudian didukung dengan penambahan data atau unsur empiris. Dalam penelitian hukum normatif, hukum yang ditulis dikaji dari beberapa aspek seperti teori, filosofi,

[14] Oktaviani Sugiarto, 2019, *"Tinjauan Hukum Internasional Terkait Perlindungan Data dan Informasi Pribadi"*, Skripsi, Sarjana Hukum, Fakultas Hukum Universitas Hasanuddin, Makassar.

perbandingan, struktur/komposisi, konsistensi, penjelasan umum dan penjelasan pada tiap pasal, formalitas, dan kekuatan mengikat suatu undang-undang serta bahasa yang digunakan adalah bahasa hukum. Sedangkan,

2. Jenis dan Sumber Bahan Penelitian

a. Jenis Bahan Hukum

Jenis bahan hukum yang digunakan dalam penulisan proposal ini, yaitu:

1) Bahan hukum primer, yaitu bahan yang diperoleh dari peraturan tertulis yang ditegakkan negara, konvensi-konvensi atau putusan kasus yang relevan dengan pokok pembahasan penelitian ini.
2) Bahan hukum sekunder, yaitu bahan yang diperoleh dari literaturliteratur seperti buku, hasil penelitian, jurnal ilmiah yang relevan dengan pokok pembahasan dalam penelitian ini.
3) Bahan hukum tersier, yaitu bahan non-hukum merupakan bahan yang memberikan petunjuk maupun penjelasan sebagai pelengkap atas bahan hukum primer dan sekunder yang antara lain Kamus Bahasa Indonesia, Kamus Hukum, surat kabar, majalah, serta bahan-bahan yang ada di internet dan wawancara narasumber/ahli sesuai dengan permasalahan yang teliti.[15]

[15] Jonaedi Efendi dan Johnny Ibrahim, 2016, *Metode Penelitian Hukum Normatif dan Empiris*, Kencana, Jakarta hlm. 16

b. Sumber Bahan Hukum

Adapun sumber bahan hukum yang akan menjadi sumber informasi/referensi penulis dalam melakukan penelitian ini adalah:

1) Ketentuan-ketentuan Hukum Internasional dan Hukum Nasional;
2) Buku-buku yang berkaitan dengan pokok pembahasan dalam penelitian ini;
3) Literatur-literatur lain seperti hasil penelitian, jurnal ilmiah, media pemberitaan, dan data-data lainnya yang diperoleh yang relevan dengan pokok pembahasan dalam penelitian ini.

3. Teknik Pengumpulan Bahan Hukum

Teknik pengumpulan bahan hukum yang digunakan penulis dalam penelitian ini adalah teknik studi literatur (literature research), yang ditujukan untuk memperoleh bahan-bahan dan informasi-informasi sekunder yang diperlukan dan relevan dengan pokok pembahasan penelitian, yang bersumber dari konvensi-konvensi, buku-buku, media pemberitaan, jurnal penelitian, serta sumber-sumber informasi lainnya seperti data yang terdokumentasi melalui situs internet yang relevan. Dari penelitian kepustakaan ini diharapkan diperoleh landasan teori mengenai kajian dan analisis permasalahan yang dibahas dalam penelitian ini dan perspektif hukum internasional.

4. Analisis Bahan Hukum

Penelitian ini adalah penelitian normatif yang dimana penulis memperoleh bahan hukum yang dibutuhkan diperoleh dari tinjauan kepustakaan yang bersumber dari buku-buku dan literatur lain yang relevan dengan pokok pembahasan dalam penelitian penulis. Keseluruhan bahan hukum yang diperoleh dianalisis dengan menggunakan metode analisis kualitatif dan analisis isi (content analysis), dan selanjutnya ditulis secara deskriptif.

BAB II

TINJAUAN PUSTAKA DAN ANALISIS PERMASALAHAN PERTAMA

A. Hukum Pidana Internasional

1. Definisi Hukum Pidana Internasional

Istilah Hukum Pidana Internasional atau *International Criminal Law* atau *Internationale Straffprocessrecht* semula diperkenalkan dan dikembangkan oleh pakar-pakar hukum internasional dari Eropa daratan dan Amerika Serikat.[16] Pengembangan Hukum Pidana Internasional sebagai salah satu cabang ilmu hukum dimulai oleh Gerhard O.W. Mueller dan Edmund M. Wise dengan menulis karya tulis *International Criminal Law* (1965), kemudian dilanjutkan oleh Bassiouni dan V. Nanda dengan menulis karya tulis *A Treatise on International Criminal Law* (1973).[17]

Kehadiran Hukum Pidana Internasional sebagai suatu cabang ilmu hukum baru telah memperoleh reaksi dari para pakar hukum internasional. Menurut George Schwarzenberger,[18] ada enam pengertian tentang Hukum Pidana Internasional, yaitu:

a) Hukum Pidana Internasional dalam arti lingkup territorial hukum pidana nasional (*international law in the meaning of the territorial scope of municipal criminal law*), artinya Hukum Pidana Internasional yang memiliki lingkup kejahatan-kejahatan yang melanggar kepentingan masyarakat internasional, akan tetapi kewenangan melaksanakan penangkapan, penahanan, dan peradilan atas pelaku-pelakunya diserahkan sepenuhnya kepada

[16] Romli Atmasasmita, 2003, *Pengantar Hukum Pidana Internasional*, Refika Aditama, Bandung, hlm. 19.
[17] *Ibid*.
[18] *Ibid*., hlm. 21.

yurisdiksi kriminil Negara yang berkepentingan dalam batas-batas territorial Negara tersebut.

b) Hukum Pidana Internasional dalam arti aspek internasional yang ditetapkan sebagai ketentuan dalam hukum pidana nasional (*international criminal law in the meaning of internationally prescribed municipal criminal law*), artinya Hukum Pidana Internasional ini adalah menyangkut kejadian-kejadian dimana suatu negara yang terikat pada hukum internasional berkewajiban memperhatikan sanksi-sanksi atau tindakan perorangan sebagaimana ditetapkan di dalam hukum pidana nasionalnya.

c) Hukum Pidana Internasional dalam arti kewenangan internasional yang terdapat di dalam hukum pidana nasional (*international criminal law in the meaning internationally authorized municipal criminal law*), artinya Hukum Pidana Internasional ini adalah ketentuan-ketentuan di dalam hukum internasional yang memberikan kewenangan atas negara nasional untuk mengambil tindakan atas tindak pidana tertentu dalam batas yurisdiksi kriminilnya dan memberikan kewenangan pula kepada negara nasional untuk menerapkan yurisdiksi kriminil diluar batas teritorialnya terhadap tindak pidana tertentu, sesuai dengan ketentuan-ketentuan di dalam hukum internasional.

d) Hukum Pidana Internasional dalam arti ketentuan hukum pidana nasional yang diakui sebagai hukum yang patut dalam kehidupan masyarakat bangsa yang beradab (*international criminal law in the meaning of municipal criminal law common to civilized nations*), artinya hukum pidana internasional adalah ketentuan-ketentuan di dalam hukum pidana nasional yang dianggap sesuai atau sejalan dengan tuntutan kepentingan masyarakat internasional.

e) Hukum Pidana Internasional dalam arti kerja sama internasional dalam mekanisme administrasi peradilan pidana nasional (*international criminial law in the meaning of international cooperation in the administration of municipal criminal justice*), artinya Hukum Pidana Internasional adalah semua aktivitas atau kegiatan penegakan hukum pidana nasional yang memerlukam kerja sama antarnegara, baik bersifat bilateral maupun multilateral.

f) Hukum Pidana Internasional dalam arti materiil (*international criminal law in the material scene of the world*), artinya Hukum Pidana Internasional adalah objek pembahasan dari hukum pidana internasional yang telah ditetapkan oleh PBB sebagai kejahatan internasional dan

merupakan pelanggaran atas *de iure gentium*, seperti: *piracy, genocide,* agresi, dan kejahatan perang.

2. Sumber Hukum Pidana Internasional

Dasar-dasar hukum dalam menentukan suatu perbuatan sebagai kejahatan internasional dilihat dari sumber-sumber hukum internasional bahwa sumber hukum dalam arti formal dari hukum pidana internasional yang berasal dari hukum internasional adalah kaidah-kaidah dan prinsip-prinsip hukum internasional yang berkenaan dengan kejahatan. Seperti halnya dengan sumber hukum internasional dalam arti formal pada umumnya, secara lebih spesifik sumber hukum pidana internasional dalam arti formal yang berasal dari hukum internasional yang berkenaan dengan suatu kejahatan adalah sebagai berikut:

a. Perjanjian Internasional (Traktat/*Treaty*)

Perjanjian internasional yang merupakan sumber dari hukum pidana internasional dalam arti formal, dibatasi pada perjanjian-perjanjian internasional yang substansinya baik secara langsung ataupun tidak langsung berkenaan dengan masalah kejahatan. Adanya perjanjian yang lingkupnya internasional merupakan upaya dalam menanggapi permasalahan internasional (kejahatan atau tindak pidana) karena menyangkut kepentingan negara yang satu dengan negara lainnya baik dalam skala bilateral, regional, multilateral

dan global. Namun demikian, perjanjian-perjanjian (*treaties*) yang menjadi sumber hukum internasional dapat berfungsi jika sudah mendapatkan pengakuan/dipakai oleh badan-badan atau bangsa-bangsa sebagai suatu badan (lembaga).[19]

b. Hukum Kebiasaan Internasional (*International Custom*)

Kaidah-kaidah hukum pidana internasional yang berbentuk hukum kebiasaan internasional, sebagai contoh antara lain adalah kaidah-kaidah hukum mengenai ekstradisi; yurisdiksi kriminal negara-negara berdasarkan hukum internasional. Salah satu sumber hukum internasional yaitu hukum kebiasaan internasional yang pada abad 20-an masih menjadi sumber hukum yang penting. Namun, makna Hukum Kebiasaan Internasional semakin kecil sebagai akibat yang ditimbulkan oleh semakin banyaknya dan bertambah traktat-traktat yang membentuk hukum (*law making*).[20]

c. Putusan Badan-badan Pennyelesaian Sengketa Internasional (*International Jurisprudence*)

Keputusan-keputusan badan penyelesaian sengketa internasional (pengadilan) baik internasional maupun nasional (dari berbagai negara) yang membuktikan adanya kaidah hukum internasional mengenai suatu persoalan yang dapat diselesaikan berdasarkan sumber-sumber hukum internasional

[19] Anis Widyawati, 2014, *Hukum Pidana Internasional*, Sinar Grafika, Jakarta, hlm. 16-17.

[20] *Ibid*., hlm. 20.

yang primer. Adapun beberapa keputusan yang dikeluarkan oleh badan pengadilan internasional seperti keputusan-keputusan Mahkamah Internasional permanen (*Permanent Court of International*), Mahkamah Internasional (*International Court of Justice*), Mahkamah Militer Internasional di Nuremberg 1945, Mahkamah Internasional di Tokyo 1946, dan lain-lain.[21]

d. Keputusan atau Resolusi Organisasi Internasional

Dalam bidang hukum pidana internasional, beberapa organisasi internasional baik yang universal, regional, ataupun khusus, mengeluarkan keputusan atau resolusi yang substansinya berkenaan dengan masalah kejahatan. Sifat atau keputusan dari resolusi yang dikeluarkan oleh organisasi internasional mengikat bagi negara-negara yang menjadi peserta (anggota) dari organisasi internasional tersebut. Kemudian daripada itu, banyak juga keputusan atau resolusi yang merupakan perumusan kaidah-kaidah hukum kebiasaan internasional menjadi sumber hukum yang progresif dengan melihat perkembangan kehidupan negara-negara di dunia dari hukum pidana internasional itu sendiri.[22]

e. Prinsip-prinsip Hukum Umum (General Principle)

[21] *Ibid*., hlm. 22.
[22] *Ibid*., hm. 23.

Prinsip-prinsip atau asas-asas hukum umum dalam hukum internasional maupun nasional yang berlaku untuk setiap waktu di semua tempat bagi semua negara (bangsa) yang bersifat universal, berlaku juga bagi hukum pidana internasional sebagai suatu sistem hukum dan sumber hukum. Pasal 38 Piagam Mahkamah Internasional menerangkan bahwa asas-asas hukum umum yang diakui oleh negara-negara atau bangsa-bangsa yang beradab sebagai sumber hukum internasional. Asas-asas hukum umum ini digunakan oleh Mahkamah Internasional, apabila sumber-sumber utama hukum internasional tidak mencukupi untuk dijadikan sebagai landasan hukum bagi putusan yang akan dikeluarkan oleh Mahkamah Internasional dalam menangani perkara yang menjadi kompetensinya untuk mengadili dan memutus kejahatan internasional tersebut.[23]

3. Karakteristik Tindak Pidana Internasional

Sampai saat ini belum terdapat satu pun ketentuan di dalam hukum internasional, baik dalam perjanjian-perjanjian internasional maupun dalam kebiasaan internasional yang menetapkan istilah *"international crimes".* Perdebatan mengenai peristilahan ini disebabkan pengertian istilah *"international crime"* telah membawa dampak yang lebih luas, tidak hanya

[23] *Ibid*., hlm. 23-24.

sekadar pengubahan substansi melainkan menyangkut masalah siapa yang dapat dipertanggungjawabkan dalam hal terjadinya *"international crimes"* tersebut, apalagi pelakunya tidak hanya orang perorangan atau kelompok melainkan sebuah negara merdeka dan berdaulat.

Terdapat dua pengertian yang berbeda antara *international delinquencies* dan *international crime*. *International delinquencies* diakui di dalam hukum kebiasaan internasional dan pengertian *international crimes* berkaitan dengan struktur hukum internasional. *International delinquencies* bukan merupakan suatu kejahatan, karena negara yang dianggap delinkuen tidak dapat dihukum dan sekalipun pertanggungjawaban dapat dipaksa hanyalah sebatas untuk memperbaiki tindakan yang tidak benar. Negara-negara berdaulat telah mengesampingkan kemungkinan penjatuhan pidana atas negara karena melakukan tindakan yang tidak benar.[24]

Menurut Bassiouni, *international crime* adalah setiap tindakan yang ditetapkan di dalam konvensi-konvensi multilateral dan diikuti oleh sejumlah tertentu negara-negara peserta, meskipun di dalamnya terkandung salah satu dari

[24] Romly Atmasasmita, *Op Cit*., hlm. 35.

kesepuluh karakteristik pidana. Sepuluh karakteristik pidana menurut Bassiouni[25] tersebut adalah:

a. Pengakuan secara eksplisit tindakan-tindakan yang dipandang sebagai kejahatan berdasarkan hukum internasional;
b. Pengakuan secara implisit sifat-sifat pidana dari tindakan-tindakan tertentu dengan menetapkan suatu kewajiban untuk menghukum, mencegah, menuntut, menjatuhi hukuman atau pidananya;
c. Kriminalisasi terhadap tindakan yang dilarang;
d. Hak dan kewajiban untuk menuntut;
e. Hak dan kewajiban untuk memberikan hukuman terhadap tindakan yang dilarang;
f. Hak dan kewajiban untuk mengekstradisi;
g. Hak dan kewajiban untuk bekerja sama dalam penuntutan, penghukuman termasuk bantuan yudisial di dalam proses penghukuman;
h. Penetapan dasar-dasar yurisdiksi kriminal;
i. Referensi pembentukan suatu pengadilan pidana internasional;
j. Penghapusan alasan-alasan perintah atasan.

[25] *Ibid.*, hlm. 37-38.

Terdapat beberapa ciri pokok yang dapat membedakan suatu perbuatan atau tindakan itu merupakan tindak pidana internasional atau bukan. Ciri pokok tersebut adalah tindakan tersebut harus mengandung unsur transnasional dan/atau internasional serta harus diukur apakah mengandung unsur *necessity* (kebutuhan). Tindakan tersebut harus memenuhi persyaratan-persyaratan sebagai pelanggaran terhadap kepentingan masyarakat bangsa-bangsa atau masyarakat internasional dan memenuhi persyaratan bahwa tindakan pidana tersebut memerlukan penanganan secara internasional sehingga setiap negara berhak dan berkewajiban untuk menangkap, menahan, dan menuntut, serta mengadili pelaku kejahatan dimanapun itu dilakukan.

B. Kejahatan Siber

1. Definisi Kejahatan Siber

Berbicara masalah kejahatan siber tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalu dimutakhirkan

sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan siber ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Untuk lebih mendalam ada beberapa pendapat di bawah ini tentang apa yang dimaksud dengan kejahatan siber. Diantaranya adalah menurut Kepolisian Inggris, kejahatan siber adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.[26]

Menurut Peter Stephenson,[27] kejahatan siber adalah:

> *"The easy definition of cyber crime is crimes directed at a computer or a computer system. The nature of cyber crime, however, is far more complex. As we will see later, cyber crime can take the form of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system."*

Dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief,[28] mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana, Kuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian kejahatan siber, yaitu *cybercrime* dan *computer related crime*.

---

[26] Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Jakarta, hlm. 40.

[27] Peter Stephenson, 2000, *Investigating Computer Related Crime: A Hanbook For Corporate Investigators,* London New York Washington D.C., CRC Press, hlm. 56.

[28] Barda Nawawi Arief, 2007, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Predana Media Group, Jakarta, hlm. 24.

Dalam *background paper* untuk lokakarya Kongres PBB X/2000 di Wina, Austria, istilah kejahatan siber dibagi dalam dua kategori. Pertama kejahatan siber dalam arti sempit (*in a narrow sense*) disebut *computer crime*. Kedua, kejahatan siber dalam arti luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut:

a. *Cyber crime in a narrow sense (computer sense): any legal behavior directed by means electronic operations that targets the security of computer system and the data processed by them;*
b. *Cyber crime in a broader sense (computer related crime): any illegal behavior commited by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*

Pengertian komputer dalam *The Proposed West Virginia Computer Crimes Act* adalah:[29]

> *"an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or typesetter, a portable handheld calculator, or other similar device".*

Dari pengertian kejahatan komputer menurut peraturan perundang-undangan di Virginia dapat dipahami bahwa sesuatu yang berhubungan dengan peralatan pemerosesan data listrik, magnetik, optik, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi

[29] *Anonymous*, *Cybercrime*: *Sebuah Fenomena di Dunia Maya*, diakses melalui https://www.divhubinter.polri.go.id/dhi/viewBerita.php?id=13 pada tanggal 10 November 2019 pukul 02.12 Wita.

penyimpanan dan memasukan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau *typesettter*, sebuah kalkulator tangan atau peralatan serupa lainnya.[30] Secara garis besarnya, kejahatan siber dapat diartikan sebagai sebuah perbuatan melawan hukum dimana komputer sebagai alat atau sebagai target maupun keduanya.[31]

2. Jenis Jenis Kejahatan Siber

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk modus operandi yang ada, antara lain:[32]

a. *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik system jaringan computer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk

[30] Abdul Wahid dan Mohammad Labib, *Op Cit*., hlm. 41.
[31] Mohamed Chawki dkk, 2015, *Cybercrime, Digital Forensic and Jurisdiction*, Switzerland, Springer, hlm. 3.
[32] Maskun, 2013, *Kejahatan Siber (Cyber Crime)*, Kencana, Jakarta, hlm.51.

mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.

b. Illegal Contents

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

c. Data Forgery

Merupakan kejahatan dengan memalsukan data pada dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan memuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalahgunakan.

d. *Cyber Espionage*

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (*database*) tersimpan dalam suatu sistem yang tersambung dalam jaringan komputer.

e. *Cyber Sabotage and Extortion*

Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*,[33] virus komputer ataupun suatu program tertentu, sehingga data program komputer atau sistem jaringan tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

f. Offense Againts Intelectual Property

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh, peniruan

[33] *Logic bomb* adalah suatu program yang dibuat dan dapat digunakan oleh pelakunya sewaktu-waktu atau tergantung dari keinginan dari si pelaku, dari situ terlihat bahwa informasi yang ada di dalam computer tersebut dapa terganggu, rusak, atau bahkan hilang.

tampilan pada *web page* suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

g. *Infringements of Privacy*

Kejahatan ini biasanya ditujukan terhadap serangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui orang lain maka dapat merugikan korban secara materil maupun inmateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Menurut *Convention on Cybercrime*, tindak pidana yang dapat digolongkan seabagai *cybercrime* diatur dalam Pasal 2-10, adapun tindak pidana tersebut adalah:

a. *Illegal Access*

Illegal access atau akses ilegal diatur dalam Pasal 2 *Convention on Cybercrime*, yang berbunyi:

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that offence be committed by infringing security measures, with the intent of obtaining computer or other dishonest intent, or in relation to a computer system that is connected to another computer system."*

Illegal access melingkupi pelanggaran dasar dari ancaman-ancaman yang berbahaya dari serangan terhadap keamanan data

dan sistem komputer.[34] Perlindungan terhadap pelanggaran *illegal access* ini merupakan gambaran dari kepentingan organisasi atau kelompok dan orang-orang yang ingin mengatur, menjalankan dan mengendalikan sistem mereka berjalan tanpa ada gangguan dan hambatan.[35]

Contoh dari akses ilegal adalah Pada tahun 2011, Audrey Aurnheimer dan Daniel Spitler dituntut atas tuduhan peretasan. Mereka berdua menemukan celah pada situs AT&T sehingga mereka dapat mengakses alamat email pengguna iPad AT&T. Mereka berdua berhasil mengumpulkan 120.000 alamat email penggunan iPad AT&T. Pemerintah Amerika Serikat mengatakan mengakses email tersebut merupakan tindak kriminal peretasan. Auernheimer dan Splitter terbukti bersalah dan divonis hukuman 3 setengah tahun penjara.[36]

b. *Illegal Interception*

Illegal interception atau penyadapan ilegal diatur dalam Pasal 3 *Convention on Cybercrime*, yang berbunyi:

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer*

[34] *Council of Europe*, *Explanatory Report to The Convention on Cybercrime* (ETS No. 185), poin ke 44.

[35] Akbar Kurnia Putra, *"Harmonisasi Konvensi Cybercrime Dalam Hukum Nasional"*. Jurnal Ilmu Hukum. Vol. 5, No. 2, Oktober 2014, hlm. 100.

[36] Kim Zetter, *AT&T Hacket 'Weev' Sentenced to 3,5 Years Prison*, diakses melalui https://www.wired.com/2013/03/att-hacker-gets-3-years/ pada tanggal 9 Januari 2020 pukul 23.18 Wita

system, including electromagnetic emissions from a computer system carrying such computer data. A party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

Menyatakan tidak sah tindakan pencegatan atau menahan tanpa hak bentuk pemindahan data komputer yang dilakukan secara pribadi yang dilakukan melalui faksimile, *email*, atau pemindahan *file*. Tujuan dari pasal ini adalah perlindungan dasar atas hak kebebasan dalam komunikasi data. Pelanggaran ini hanya ditujukan terhadap pemindahan pribadi dari data komputer.[37]

Contoh dari penyadapan ilegal adalah pada tahun 2011, Aaron Swartz didakwa oleh pengadilan Amerika Serikat setelah diduga mengakses jaringan Massachusetts Institute of Technology (MIT) dan mengunduh 2,7 juta data akademis paper yang sebenarnya tersedia gratis bagi pengunjung kampus melalui layanan Journal Storeage (JSTOR). JSTOR sendiri sebenarnya tidak mengajukan keberatan, tetapi Departemen Kehakiman Amerika Serikat tetap melakukan dakwaan, karena Swartz dianggap melanggar kebijakan layanan mengunduh dokumen dan mendistribusikannya di luar kampus. Swartz didakwa hukuman maksimal 35 tahun penjara, tetapi 3 bulan sebelum sidang putusannya Swartz melakukan bunuh diri.[38]

[37] Akbar Kurnia Putra, *Op Cit*. Hlm. 100.

[38] John Naughton, *Aaron Swartz Stood Up for Freedom and Fairness – and was Hounded to His Death*, diakses melalui https://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy pada tanggal 9 Januari 2020 pukul 23.40 Wita.

c. Data Interference

Data interception atau gangguan data diatur dalam Pasal 4 *Convention on Cybercrime* yang berbunyi:

1) *Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deteriotation alteration or suppression of computer data without right.*
2) *A party may reserve the right to require that the conduct described in Paragrapg 1 result in serious harm.*

Ketentuan pengrusakan data menjadi tindak pidana bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program komputer sebagaimana dengan benda-benda berwujud. Sebagai contoh, memasukan kode-kode jahat (*malicious codes*), virus, dan *Trojan Horse*[39] ke suatu sistem komputer merupakan pelanggaran menurut ketentuan pasal ini.[40]

Contoh dari gangguan data adalah pada tahun 1983, FBI menangkap kelompok kriminal komputer bernama The 414s yang berbasis di Milwaukee, AS. Kelompok yang kemudian disebut hacker tersebut melakukan pembobolan 60 buah komputer-komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Hal ini menyebabkan kerugian

[39] *Trojan Horse* mengacu pada program berbahaya yang muncul menyamar sebagai sesuatu program yang tidak berbahaya pada sistem komputer, seperti *file* musik atau video.

[40] Akbar Kurnia Putra, *Op. Cit.*, Hlm. 101.

bagi perusahaan Pusat Kanker Memorial Sloan-Kettering dan Laboratorium Nasional Los Alamos karena pelaku dengan sengaja merusak komputer dan data-data penting dari perusahaan yang menyebabkan kerugian finansial, bahkan merembet ke finansial negara.[41]

d. System Interference

System Interference atau gangguan sistem diatur dalam Pasal 5 *Convention on Cybercrime* berbunyi:

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriotating, altering or suppressing computer data."*

Dalam Pasal 5 konvensi ini disebutkan bahwa *system interference* ditetapkan sebagai pelanggaran pidana apabila "… *when committed intentionally, the serious hindering without right of the functioning of a computer system …*", harus dilakukan dengan memasukkan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer. Penggangguan terhadap sistem dijadikan sebagai tindak pidana bertujuan untuk mencegah "*… the serious hindering without right of the functioning of a computer system …*".[42]

---

[41] Timothy Winslow, *I Hacked Into a Nuclear Facility in '80s*, diakses melalui https://edition.cnn.com/2015/03/11/tech/computer-hacker-essay-414s/index.html pada tanggal 9 Januari 2020 pukul 23.32 Wita

[42] Akbar Kurnia Putra, *Op. Cit.* Hlm. 101.

Contoh dari gangguan sistem adalah pada tahun 2000, sebuah virus yang dinamakan "*love bug*" menyerang dan melumpuhkan 50 juta komputer dan jaringan. Virus tersebut juga menyerang komputer-komputer milik Pentagon, CIA dan organisasi-organisasi besar lainnya dan menyebabkan kerugian berjuta-juta dolar akibat kerusakan-kerusakan.[43]

e. Misuse of Device

Misuse of device atau penyalahgunaan perangkat diatur dalam Pasal 6 *Convention on Cybercrime*, adapun yang termasuk jenis kejahatan ini adalah pencurian, penyediaan, penjualan dan distribusi dari data komputer yang diperoleh dari sebuah alat. Pasal 6 berbunyi:

> *Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*
> a. *The production sale, procurement for use, distribution or otherwise making available of:*
> *i. A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 through 5;*
> *ii. A computer password, access code, or similar data by which in the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Article 2 through 5; and*
> b. *The possession of an item referred into paragraph* i or ii *above, with intent that it be used for the purpose of committing any of the offences established in Article 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches."*

[43] Mike Ingram, 'Love Bug' Virus Damaged Estamated at $10 Billion, diakses melalui https://www.wsws.org/en/articles/2000/05/bug-m10.html pada tanggal 10 Januari 2020 pukul 00.06 Wita.

Adapun yang dimaksud alat di sini adalah *hardware* maupun *software* yang telah dimodifikasi untuk mendapatkan akses dari sebuah komputer atau jaringan komputer. Contohnya apabila ada seseorang memasukkan *keylogger*[44] dalam jaringan bank untuk mendapatkan data-data nasabah mulai dari alamat sampai ke *password* ATM dan data-data tersebut dijual, digunakan atau didistribusikan untuk kejahatan lain.[45]

f. Computer-related Forgery

Computer-related Forgery atau pemalsuan yang berhubungan dengan komputer diatur dalam Pasal 7 *Convention on Cybercrime*, yang berbunyi:

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminals offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.*

Tindak pemalsuan yang dimaksud dalam pasal tersebut adalah memasukkan , mengubah, menghapus, atau menahan data komputer, sehingga menyebabkan data menjadi tidak seperti aslinya dengan maksud bahwa hal itu dianggap atau dilakukan untuk sebuah tujuan hukum tertentu seakan-akan asli, tanpa mempertimbangkan

[44] *Keylogger* adalah perangkat lunak pengintip untuk merekam apa saja yang diketikkan oleh pengguna di *keyboard*.

[45] Akbar Kurnia Putra , *Op.Cit.*, Hlm. 102.

apakah data tersebut bisa dibaca dan bisa dimengerti secara langsung.

g. Computer-related Fraud

Computer-related fraud atau penipuan yang berhubungan dengan komputer diatur dalam Pasal 8 *Convention on Cybercrime*, yang berbunyi:

> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:*
> a. Any input, alteration, deletion or suppression of computer data;
> b. Any interference with the functioning of a computer system,
> With fraudeulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Contoh dari tindakan pemalsuan yang berhubungan dengan komputer yang paling besar adalah *nigerian mail fraud*.[46] *Nigerian mail fraud* merupakan penipuan dengan megirimkan *email* kepada korbannya yang menawarkan komisi apabila bersedia membantu untuk mengeluarkan uang dari Nigeria secara illegal. Biasanya jika membalas *email* ini, korban akan mendapatkan banyak bukti yang meyakinkan, seperti lampiran dari pihak birokrasi Nigeria, bahkan lengkap dengan identitas pengiriman *email* tersebut. Kemudian jika dilanjutkan korban tersebut akan diminta untuk membantunya meloloskan uang tersebut dengan menyogok pihak yang berwenang tentunya dengan uang pribadi korban terlebih dahulu. Selanjutnya,

[46] Jonathan Clough, 2010, *Principles of Cybercrime*, United Kingdom, Cambridge, hlm. 183.

korban akan diminta mengirimkan data-data termasuk kop surat dan lain-lain yang ceritanya akan dibuat seolah-olah uang tersebut dikirim untuknya. Ketika korban menghentikan pengiriman uang, pelaku penipuan tersebut telah mendapatkan data-data pribadi lengkap termasuk nomor kartu kredit, identitas dan lain-lain. Hingga saat ini, modus *nigerian mail fraud* ini telah berkembang. Tidak hanya melalui *email* namun juga telah dilakukan di media sosial lainnya, seperti *Facebook* dengan beragam cerita yang disampaikan pelakunya.[47]

h. Offences Related to Child Pornography

Offences related to child pornography atau pelanggaran yang berkaitan dengan pornografi anak diatur dalam Pasal 9 *Convention on Cybercrime* yang berbunyi:

> *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:*
> *a. Producing child pornography for the purpose of its distribution through a computer system;*
> *b. Offering or making available child pornography through a computer system;*
> *c. Distributing or transmitting child pornography through computer system;*
> *d. Procuring child pornography through a computer system for oneself or for another person;*
> e. *Possessing child pornography in a computer system or on a computer data storage medium.*

Tindakan pornografi melalui sistem komputer yang melibatkan anak (yang dalam hal ini berumur dibawah 18 tahun) telah disepakati oleh Pihak Negara yang telah menyetujui *Convention on Cybercrime*

[47] Maskun dan Wiwik Meilarati, 2017, *Aspek Hukum Penipuan Berbasis Internet*, Keni Media, Bandung, hlm. 68-69.

sebagai kejahatan siber. Dianggapnya pornografi anak sebagai kejahatan (tidak hanya terbatas pada kejahatan siber) berbeda dengan pornografi yang dilakukan orang dewasa disebabkan karena adanya implikasi pornografi anak ini merujuk pada merekam kekerasan terhadap anak, bahkan di beberapa negara mendeskripsikan lebih akurat ke eksploitasi anak.[48]

Contoh dari pornografi anak adalah pada tahun 2017 kasus yang terjadi di Bandung, dimana tersebar 2 video porno antara perempuan dewasa dengan anak dibawah umur. Berdasarkan penyelidikan polisi terungkap bahwa yang membuat dan menyutradarai video tersebut adalah laki-laki bernama M. Faisal Akbar. Faisal mendapat tawaran dari seseorang berinisial R yang mengaku orang Kanada untuk membuat video pornografi yang melibatkan anak dibawah umur dengan imbalan bayaran uang. Atas tindakannya, Faisal divonis 7 tahun penjara serta denda sebesar Rp. 250 juta subsider 6 bulan kurungan.[49]

i. Offences Related to Infringement of Copyright and Related Rights

[48] Jonathan Clough, *Op. Cit.*, Hlm. 255.

[49] Yedi Supriadi, *Otak Pelaku Pembuatan Video Asusila Anak Divonis 7 Tahun*, diakses dari http://www.pikiran-rakyat.com/bandung-raya/2018/08/28/otak-pelaku-pembuatan-video-asusila-anak-divonis-7-tahun-429355 pada tanggal 10 Januari 2020 pukul 12.45 Wita.

Offences related to infringement of copyright and related rights atau pelanggaran yang berkaitan dengan hak cipta dan hak-hak lainnya diatur dalam Pasal 10 *Convention on Cybercrime* yang berbunyi:

1) *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.*
2) *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protectio of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Perfomances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.*

Pelanggaran pada hak cipta ini merujuk pada kegiatan yang memproduksi atau mendistribusikan karya orang lain secara ilegal atau tanpa sepengetahuan pemegang hak ciptanya. Hak cipta sendiri hanya bagian dari hak-hak kekayaan intelektual, contoh lainnya adalah hak paten, merek, dll. [50]

[50] Jonathan Clough, *Op. Cit.*, Hlm. 221.

C. Ransomware

1. Sejarah Virus *Ransomware*

Peristiwa virus *ransomware* yang pertama terjadi jauh sebelum era internet masa kini, yaitu 31 tahun yang lalu. Virus *Ransomware* pertama diciptakan oleh seorang ahli biologi bernama Joseph Popp pada tahun 1989.[51] Joseph Popp membuat sebuah perangkat lunak jahat yang disamarkan sebagai sebuah program edukasi tentang *AIDS* yang disebut *"Trojan AIDS"* dan memasukkannya ke dalam 20.000 buah disket kemudian mengirimkannya ke 90 negara di dunia melalui jasa pos. Setelah korban-korbannya memasukkan disket tersebut ke komputer dan menjalankan program yang terdapat di dalamnya, maka saat itu pula virus *Trojan AIDS* tersebut bekerja dengan mengenkripsi *file-file* yang ada dalam komputer tersebut dan meminta korban untuk membayar tebusan sebesar $189 dengan cara mengirimkannya ke nomor PO BOX beralamat di Panama jika ingin mendapat kunci dekripsinya.[52]

Istilah ransomware pertama kali disematkan pada virus *ransomware Gpcoder* pada tahun 2005. Pembuat virus *ransomware Gpcoder* menyebarkan virusnya melalui *email spam* dan korbannya bersifat acak. Virus *ransomware Gpcoder* menyerang komputer

[51] Allan Liska dan Timothy Gallo, 2017, *Ransomware: Defending Againts Digital Extortion*, Sebastopol, O'Reilly Media, Hlm. 1.

[52] Alina Simone, *The Strange History of Ransomware*, diakses melalui https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b pada tanggal 3 Januari 2020 pukul 4.38 Wita

korbannya dengan mengenkripsi data-data didalamnya dan meminta tebusan kepada korbannya jika ingin mendapat kunci dekripsinya, tetapi tidak seperti *ransomware* modern saat ini, virus *ransomware Gpcoder* masih mudah untuk ditembus dan perusahaan antivirus dapat memberikan solusi kepada pelanggan mereka yang menjadi korban untuk mendekripsi data yang disandera dalam waktu yang relatif singkat.[53]

2. Definisi Virus Ransomware

Secara harfiah *ransomware* berasal dari dua kata, yaitu *ransom* dan *malware, ransom* yang berarti tebusan dan *malware* singkatan dari *malicious software* yang berarti perangkat lunak berbahaya.[54] *Ransomware* adalah virus yang menyerang komputer maupun telepon seluler (ponsel) dengan cara melakukan enkripsi pada data komputer atau ponsel sasarannya, dimana virus ini mampu mencuri data pengguna, menghapus informasi, merusak sistem, dsb., kemudian korban harus membayar sejumlah uang tebusan jika ingin mendapatkan kunci dekripsinya. Korban biasanya dijanjikan akan memperoleh kembali data-data yang dicuri, sistem yang kembali berjalan normal, dan kembalinya informasi yang hilang. Namun, belum dapat dipastikan apakah penyerang benar-benar

[53] Ronny Richardson and Max North, *"Ransomware: Evolution, Mitigation, and Prevention"*. International Journal of Management Review. Vol. 13, No. 1, 2017, Hlm. 11.
[54] Allan Liska dan Timothy Gallo, *Op. Cit.,* Hlm. 2.

menghilangkan *ransomware* atau hanya membuat virus tersebut tidur.[55]

Tebusan-tebusan yang harus dibayarkan oleh korban tersebut pun jumlahnya bervariasi dan bentuk pembayarannya mengikuti perkembangan jaman, jika pada serangan virus *ransomware* pertama tahun 1989 tebusan dibayar dengan uang tunai dan dikirim ke alamat PO BOX tertentu, maka di masa kini tebusan tersebut dibayarkan melalui *cryptocurrency* (mata uang digital) seperti *Bitcoin* yang sulit terlacak. Dikarenakan kemampuan enkripsinya, virus *ransomware* terkenal juga dengan sebutan *cryptovirus.*[56]

D. Analisis Pengaturan Mengenai Serangan Siber Menggunakan Virus *Ransomware Wannacry* Dalam Hukum Pidana Internasional

Ransomware WannaCry adalah virus yang menyerang komputer dengan cara melakukan enkripsi pada data komputer sasarannya, dimana virus ini mampu mencuri data pengguna, menghapus informasi, merusak sistem, dan sebagainya. Cara kerja virus *Ransomware WannaCry* tergambarkan dari istilah *ransomware* itu sendiri, yaitu untuk memeras pengguna atau bisnis demi keuntungan finansial.

Virus *Ransomware WannaCry* harus mendapatkan akses ke *file* atau sistem yang akan diserangnya. Sama halnya dengan virus biologis,

[55] Muhammad Sigit Safaruddin, 2016, *Virus Komputer A-Z* , Sleman, Deepublish, Hlm. 33.
[56] *Ibid.*

sebuah virus komputer membutuh akses untuk menyerang sasarannya. Akses tersebut didapatkan melalui 3 metode, yaitu: [57]

1. *Email Attachments*
   Metode yang cukup lazim digunakan untuk mendistribusikan virus *ransomware* adalah melalui lampiran *email*. Sebuah *email* disamarkan sebagai pemberitahuan yang mendesak, contohnya pemberitahuan dari bank ke nasabahnya melalui *email* dan mengarahkan korbannya ke sebuah lampiran atau tautan yang jika dibuka isinya kosong tetapi sebenarnya lampiran atau tautan itu berisi virus *Ransomware WannaCry* dan tanpa diketahui memberikan akses ke virus tersebut untuk masuk ke sistem.
2. *Message*
   Metode lain yang digunakan oleh penyerang virus *ransomware* adalah dengan mengirimkan pesan kepada korbannya melalui media sosial. Sebuah akun palsu yang meniru "teman" korbannya dibuat untuk mengirim pesan dengan lampiran *file*. Setelah dibuka, virus *Ransomware WannaCry* dapat memperoleh akses ke sistem dan mengunci jaringan yang terhubung ke perangkat yang terinfeksi.
3. *Pop-Ups*
   Metode penyerangan virus *ransomware* lain yang umum namun lebih tua adalah iklan "pop-ups". Sebuah iklan dibuat untuk muncul di layar komputer korban ketika mengakses situs-situs tertentu dengan maksud memancing korban untuk meng-klik tautan yang dilampirkan di iklan tersebut sehingga korban akan mengikuti petunjuk-petunjuk yang tersedia yang ternyata dirancang untuk mendistribusikan virus *Ransomware WannaCry* ke sistem komputer korbannya.

Tujuan dari serangan virus *Ransomware WannaCry* rata-rata sama, yaitu menargetkan uang tebusan dari korbannya. Dengan skema yang cukup mudah, yaitu melancarkan serangan secara acak dan menunggu tebusan dari korbannya untuk mendapatkan kembali datanya. Mirip dengan kasus-kasus *hacking* lainnya, dimana penyerang harus masuk ke

[57] Juliana De Groot, A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, diakses melalui https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time pada tanggal 10 Januari 2020 pukul 4.09 Wita.

komputer target, mencuri data yang diinginkan, mencari pembeli untuk data itu, menegosiasikan kesepakatan, dan memproses pembayaran. Namun, dalam beberapa kasus dapat memakan waktu berminggu-minggu atau berbulan-bulan, dengan asumsi korban bersedia membayar untuk data yang dicuri.[58] Hal tersebut sejalan dengan hasil wawancara penulis dengan salah satu *hacker* terdaftar di Indonesia yakni Samsaraji Bunayya bahwa tujuan dari *hacker* untuk menyerang menggunakan virus *ransomware* adalah untuk memperoleh data dari korban yang nantinya akan ditebus, yang pada umumnya ditebus menggunakan *bitcoin*.[59]

Selain *Ransomware WannaCry,* virus *ransomware* juga terdapat dalam beberapa jenis, yaitu:

1. Ransomware CryptoLocker

Ransomware CryptoLocker adalah salah satu jenis *ransomware* yang pernah menyebar di dunia pada bulan September 2013 sampai bulan Mei 2014 yang menyerang komputer pribadi dan perusahaan. Seperti *ransomware* pada umumnya, *ransomware CryptoLocker* ini mengenkripsi data-data pada sistem komputer sasarannya dan menampilkan pesan di layar monitor komputernya untuk membayar sejumlah uang tebusan.

Untuk mengatasi *Ransomware CryptoLocker* tersebut, sejumlah perusahaan keamanan siber mengambil contoh data dari komputer-komputer yang terinfeksi oleh *ransomware CryptoLocker* untuk

[58] Allan Liska dan Timothy Gallo, *Op. Cit.,* Hlm. 28.
[59] Wawancara Samsaraji Bunayya, *Hacker* terdaftar di Indonesia, Online, 20 Agustus 2021.

diteliti lebih lanjut mengenai virus tersebut, hingga akhirnya pada bulan Juli 2014 para ahli berhasil membuat antivirus untuk mengatasinya dan antivirus tersebut dapat diakses secara umum dan gratis oleh masyarakat melalui *website* khusus.[60] Diperkirakan kerugian dari serangan *ransomware CryptoLocker* ini mencapai $ 3 juta dengan jumlah korban sebanyak 250.000 sistem komputer.[61]

Berdasarkan penyelidikan FBI, sebuah kelompok yang bernama *GameOver Zeus* yang berbasis di Rusia dan Ukraina bertanggung jawab atas pembuatan dan penyebaran *Ransomware Cryptolocker* ini serta telah mengidentifikasi seorang pria berkebangsaan Rusia bernama Evgeniy Mikhailovich Bogachev sebagai pimpinannya. Sebagai upaya untuk menangkapnya dibuatlah sebuah operasi gabungan yang disebut *Operation Tovar* yang terdiri dari agensi penegak hukum pemerintah seperti FBI dan Europol bersama dengan perusahaan keamanan siber swasta dan juga peneliti-peneliti dari universitas, tetapi sampai sekarang Evgeniy Mikhailov Bogachev belum berhasil ditangkap tetapi diyakini dia berada di negara Rusia.[62]

2. Ransomware Cryptowall

---

[60] Mark Ward, *CryptoLocker Victims to Get Files Back for Free*, diakses melalui https://www.bbc.com/news/technology-28661463 pada tanggal 16 Maret 2021 pukul 17.04 Wita.

[60]Toshima Singh Rajput, "*Evolving Threat Agents: Ransomware and their Variants",*International Journal of Computer Application, Vol. 164, No. 7, April 2017, Hlm. 30.

[61] *Ibid.*

[62] Anonim, *GameOver Zeus Botnet Disrupted*, diakses melalui https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted pada tanggal 16 Maret 2021 pada pukul 22.46 Wita

Ransomware Cryptowall pertama kali muncul pada akhir bulan Februari 2014 dan sejak itu banyak versinya telah muncul. *Cryptowall* diyakini sebagai bentuk baru dari CryptoLocker karena versi pertama dari *ransomware* ini, yaitu *Cryptowall* 1.0 memiliki kemiripan dengan *CryptoLocker* dari segi bentuk dan penampakan. Versi 2.0-nya memiliki banyak saluran penyebaran seperti melalui lampiran *email*, *drive-by download*,[63] *exploit kit*,[64] dan *pdf* berbahaya. Virus ini juga menambahkan penggunaan jaringan *The Onion Router* (TOR) untuk komunikasi ke server kontrol. Versi 3.0 menggunakan teknik eskalasi premium dan jaringan *peer to peer* lainnya yang disebut jaringan *Invisible Internet Project* (I2P) yang merupakan jaringan yang unggul karena dinamikanya.[65]

Menurut FBI, *Cryptowall* adalah salah satu serangan siber yang paling banyak terjadi pada tahun 2015 di Amerika Serikat yang digunakan oleh banyak penjahat siber untuk menyerang individu maupun bisnis dan meminta tebusan sebesar $200 sampai $10.000 ke korbannya. Banyaknya serangan siber yang menggunakan varian *ransomware* ini dikarenakan *ransomware* ini diperjualbelikan di *darkweb* sehingga dapat dibeli oleh pihak manapun. Hingga saat ini, diketahui versi paling baru dari *Ransomware Cryptowall* bernama

[63] *Drive-by download* adalah proses pengunduhan virus, malware, atau *worm* yang dilakukan secara otomatis oleh komputer tanpa sepengetahuan pemiliknya ketika memasuki *website*, lampiran *e-mail* atau *link*, atau membuka iklan *pop-up* tertentu.

[64] *Exploit kit* adalah seperangkat program yang digunakan penjahat siber untuk membobol masuk ke sistem komputer yang lemah dan menyebarkan virus kedalamnya.

[65] Toshima Singh Rajput, *op cit.* Hlm. 31.

Cryptowall 4.0. Meskipun *Ransomware Cryptowall* terus menerus berevolusi dan diperjualbelikan tetapi pihak perusahaan antivirus pun tetap melakukan pembaruan terhadap program pertahanan virus mereka sehingga dapat menahan jika sewaktu-waktu *Ransomware Cryptowall* ini menyerang.

3. Ransomware REvil

Serangan siber menggunakan *Ransomware REvil* merupakan serangan siber yang masih tergolong baru karena terjadi pada tahun 2021. *Ransomware REvil* atau yang disebut *Sodinokibi* adalah *ransomware* yang dibuat dan disebarkan oleh kelompok *hacker* bernama *DarkSide*. Kelompok ini sulit untuk dilacak dikarenakan setiap pelacakan yang dilakukan oleh pihak berwenang selalu menemukan titik lokasi yang berbeda-beda, hal ini diyakini karena kelompok ini saling melindungi lokasi anggotanya satu sama lain sehingga ketika dilakukan pelacakan maka akan menampilkan titik lokasi yang berbeda-beda. Meskipun mengalami kendala dalam melakukan pelacakan terhadap kelompok *DarkSide* ini, tetapi diperkirakan kelompok ini berasal dari Rusia dikarenakan *ransomware* ini tidak pernah menyerang organisasi-organisasi Rusia atau negara-negara bekas Uni Soviet.[66]

Dalam menindak kelompok ini dibuatlah sebuah operasi yang dinamakan *Operation GoldDust* yang melibatkan 17 negara, Europol,

[66] Juha Saarinen, *No Let Up on REvil Ransomware as a Service Attack*, diakses melalui https://www.itnews.com.au/news/no-let-up-on-revil-ransomware-as-a-service-attacks-537189 pada tanggal 2 Agustus 2021

Eurojust, dan *Interpol*. Dalam operasi itu berhasil menangkap lima orang yang terindikasi berhubungan dengan *ransomware REvil* dan serangan *ransomware* lainnya. Mereka dituduh melakukan 5000 serangan dan berhasil mengumpulkan uang sekitar setengah juta euro yang merupakan bayaran tebusan dari *ransomware*.[67] Pemerintah Amerika Serikat dalam hal ini Departemen Kehakiman Amerika Serikat menjatuhkan dakwaan kepada salah dua dari lima tersangka itu, yakni warga negara Ukraina bernama Yaroslav Vasinskyi dan warga negara Rusia bernama Yevgeniy Polyanin. Departemen Kehakiman Amerika Serikat bekerja sama dengan Kepolisian Nasional Ukraina dalam menentukan dakwaannya, yaitu mendakwa Vasinskyi hukuman penjara selama 115 tahun dan Polyanin hukuman penjara selama 145 tahun.[68]

Walaupun virus r*ansomware* terdapat berbagai jenis, tetapi pada umumnya sifat dan cara kerjanya tetap sama, yaitu mengenkripsi data-data dalam sistem komputer sasarannya dan meminta uang tebusan kepada korban jika ingin datanya kembali.

Dalam beberapa kepustakaan, kejahatan siber atau *cybercrime* sering diidentikkan sebagai *computer crime*. Menurut *Organization for Economic Cooperation Development* (OECD) yang menggunakan istilah

[67] Europol Press Release, *Five Affiliate to Sodinokibi/REvil Unplugged*, diakses melalui https://www.europol.europa.eu/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged pada tanggal 2 Agustus 2021

[68] Anonim, *Ukrainian Arrested and Charged with Ransomware Attack on Kaseya*, diakses melalui https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya pada tanggal 2 Agustus 2021

computer related crime berarti : "*Any illegal, unethical or unauthorized behavior involving automatic data processing and / or transmission file*." (segala tindakan ilegal, tidak sah ataupun tidak etis yang berhubungan dengan pengolahan suatu data atau juga transmisi data). Berdasarkan pengertian yang telah disebutkan, maka dapat dirumuskan bahwa *computer related crime* merupakan perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.[69]

Kejahatan siber di sisi lain, bukan hanya menggunakan kecanggihan teknologi komputer, akan tetapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya. Hal ini dapat dilihat pada literatur yang dikemukakan oleh Indra Safitri yang mengemukakan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakterisitik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[70]

Dalam menentukan serangan virus menggunakan *Ransomware WannaCry* sebagai suatu bentuk kejahatan siber, maka hal tersebut perlu ditinjau dari regulasi hukum internasional yang mengatur terkait kejahatan

---

[69] Maskun, 2013, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*, Kencana Prenada Media Group, Jakarta, hlm. 46.

[70] T Mhd Aulia Fitra, "*Tinjauan Hukum Internasional Atas Perbuatan Hacking Dan Cracking Sebagai Bentuk Dari Kejahatan Cybercrime"*, Skripsi, Fakultas Hukum Universitas Sumatera Utara, Medan, 2018, hlm. 15.

siber. Meskipun secara spesifik dalam regulasi hukum internasional tidak menyebutkan secara detail terkait serangan virus menggunakan *Ransomware WannaCry*, namun hal tersebut dapat ditinjau dengan beberapa indikator yang menjadi dasar dalam menentukan kejahatan siber tersebut.

Adapun regulasi hukum internasional yang mengatur mengenai kejahatan siber termasuk kejahatan melalui virus *Ransomware WannaCry* diawali pada tahun 1990-an di beberapa negara di sebagian belahan dunia sudah mulai mengatur mengenai kejahatan siber seperti memasuki sistem komputer secara ilegal, merusak data sistem komputer dan menyebarkan virus. Untuk menghadapi ancaman dan bahaya dari perbuatan kejahatan siber, masyarakat internasional pun membahas permasalahan kejahatan siber ini melalui forum-forum internasional. Hasil dari pembahasan itu melahirkan sejumlah regulasi internasional yang khusus membahas kejahatan siber. Regulasi siber internasional tersebut, yaitu :

1. Perserikatan Bangsa-Bangsa (PBB)

   Perserikatan Bangsa-Bangsa (PBB) telah melakukan pengawasan terhadap perkembangan *computer related crime*. Dimulai pada tahun 1990 dengan *Eighth UN Congress on the Prevention of Crime and Treatment of Offender* di Havana, Kuba pada 27 Agustus – 7 September 1990. Dalam Resolusi Kongres PBB tersebut, negara-negara dihimbau untuk mengintensifkan usaha-

usaha untuk memerangi *computer related crime* dengan melakukan tindakan-tindakan berikut:[71]

a. Modernisasi hukum pidana materil dan hukum acara pidana nasional termasuk upaya-upaya untuk (1) menjamin memadainya penerapan hukum yang ada mengenai tindak pidana dan kewarganegaraan investigasi dan pembuktian dalam proses peradilan, dan apabila diperlukan melakukan perubahan yang diperlukan. (2) Apabila tidak ada aturan yang dapat diterapkan membuat aturan tentang tindak pidana serta prosedur investigasi dan pembuktian, apabila diperlukan untuk mengatasi aktivitas kriminal yang baru dan canggih ini. (3) Kewenangan untuk menyita atau mengembalikan aset-aset hasil kejahatan yang berkaitan dengan komputer.
b. Meningkatkan upaya-upaya pengamanan komputer dan upaya-upaya preventif, dengan memperhitungkan masalah-masalah terkait perlindungan privasi, penghormatan hak asasi manusia dan kebebasan-kebebasan fundamental serta setiap mekanisme pengaturan penggunanan/pemanfaatan komputer.
c. Mengadopsi upaya-upaya agar masyarakat, aparat pengadilan dan penegak hukum peka terhadap masalah *computer-related crimes* dan pentingnya mencegah tindak pidana tersebut.
d. Mengadopsi pelatihan-pelatihan yang memadai untuk hakim, pejabat dan aparat yang bertanggungjawab atas pencegahan, penyidikan, penuntutan dan pengadilan mengenai tindak pidana ekonomi dan *computer-related crimes.*
e. Mengelaborasi dalam kolaborasi dengan organisasi-organisasi yang berkepentingan (*rules of etics*) dalam penggunaan komputer dan mengajarkannya sebagai bagian dari kurikulum dan latihan informatika
f. Mengadopsi kebijakan-kebijakan untuk korban *computer-related crimes* yang konsisten dengan *United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power*, termasuk restitusi/pengembalian aset yang diperoleh dari kejahatan, dan upaya-upaya untuk mendorong korban agar mau melaporkan kejahatan kepada penguasa yang berwenang.

[71] *Ibid*., hlm. 26-28.

Kongres PBB di Havana tersebut juga merekomendasikan kepada *Comittee on Crime Prevention and Control* untuk memajukan usaha-usaha internasional dalam mengembangkan dan menyebarluaskan pedoman dan standard kerangka kerja yang komprehensif untuk membantu negara anggota menghadapi *computer-related crimes*.[72] Pada tahun 2000 PBB menyelenggarakan *The Tenth UN Congress on The Prevention on Crime and the Treatment of Offender* di Vienna dengan tema "*Crime and Justice, meeting the challenges of the 21st century"* yang menghasilkan beberapa kesimpulan yaitu :[73]

a. *Computer related crime should be criminalized* (Kejahatan yang terkait dengan komputer harus dikriminalisasi;
b. *Adequate procedural laws were needed for the investigation and prosecution of cyber criminal* (Diperlukan hukum acara pidana yang memadai untuk melakukan penyidikan dan penuntutan terhadap pelaku tindak pidana siber;
c. *Goverment and industry should work together towards the common goal of preventing and combating computer crime so as to make the internet a secure place* (harus ada kerjasama antara pemerintah dan industri untuk mencapai tujuan bersama pencegahan dan pemberantasan kejahatan komputer agar internet menjadi tempat yang aman;
d. *Improved international cooperation was needed in order to trace criminals on the internet* (perlu peningkatan kerjasama internasional untuk melacak pelaku perbuatan kejahatan siber*)*;

[72] Perkembangan *cybercrime* telah di bahas di berbagai forum Internasional. Kongres PBB Mengenai "The Preventions of Crime and The Treatment of Offenders" (yang sejak Kongres XI berubah menjadi Congress on Cyber Prevention and Criminal Justice) telah membahas masalah cybercrime sebanyak tiga kali, yaitu pada kongres VIII/1990 di Havana, Kongres X/2000 di Wina, dan terakhir pada kongres XI/2005 di Bangkok, Sigid Suseno, *Yuridiksi Tindak Pidana Siber*, Refika Aditama, Bandung, 2012, hlm. 105.

[73] United Nations, *Tenth United Nations Congress on The Prevention of Crime and the Treatment Offenders*,Vienna, A/CONF.187/15,10-17 April 2000, hlm. 27

e. *The united Nations should take the further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks*. (PBB harus mengambil langkah lebih lanjut yang berhubungan dengan bantuan dan kerjasama teknis dalam pemberantasan *computer related crime*.

PBB mengeluarkan *International Review of Criminal Policy – United Nation Manual on the Prevention and Control of Computer-Related Crime* pada tahun 1994 sebagai bentuk tindak lanjut dari Resolusi PBB 45/121. *International review* ini memberikan pedoman kepada tiap negara mengenai substansi hukum pidana yang diatur dalam hukum nasional negara anggota, termasuk pelanggaran privasi. Berdasarkan pedoman tersebut, kejahatan komputer yang terjadi adalah:[74]

a. Penipuan melalui manipulasi dengan menggunakan sarana komputer;
b. Pemalsuan dengan menggunakan komputer;
c. Perusakan atau modifikasi terhadap data atau program komputer;
d. Pengaksessan sistem atau layanan komputer secara tanpa hak; dan
e. Reproduksi atau penggadaan secara tanpa hak terhadap program komputer yang dilindungi secara hukum.

Usaha lain yang dilakukan PBB adalah melaksanakan *A United Nation Symposium on The Challenge of Borderless Cyber-Crime*, yang dilaksanakan berkaitan dengan penandatanganan *Palermo Convention Against Transnasional Organized Crime* (UNCATOC), pada Desember 2000. Palermo Convention 2000 tidak secara khusus

[74] *Ibid*., hlm. 125

mengatur tindak pidana siber namun dalam konvensi tersebut berisi ketentuan yang mengatur kerjasama internasional cukup luas yang mencakup banyak manifestasi dari kejahatan berteknologi tinggi yang paling umum.[75] Menurut Pasal 3 ayat (2) *United Nations Convention Against Transnational Organized Crime*, suatu kejahatan dapat dikategorikan sebagai kejahatan transnasional apabila:

a. *It is commited in more than one state* (dilakukan di lebih dari satu negara);
b. *It is commited in one state but a substansial part of its preparation, planning, direction or control takes place in another state* (dilakukan di satu Negara tetapi persiapan, perencanaan, pengarahan atau pengendaliannya terjadi di negara lain);
c. *It is commited in one state but involves an organized criminal group that engages in criminal activities in more than one state*(dilakukan di satu Negara tetapi melibatkan kelompok kriminal yang terorganisir yang terlibat dalam kegiatan kriminal di lebih dari satu negara atau); *or*
d. *It is commited in one state but has substansial effects in another state* (dilakukan di satu negara tetapi memiliki dampak kerugian di negara lain).

John Broome juga mencoba menyebutkan beberapa kejahatan yang diantaranya termasuk kejahatan transnasional, yakni:[76]

a. Pelanggaran cukai;
b. Pemalsuan cukai;
c. Ekspor dan impor hewan liar;
d. Pelanggaran properti intelektual yang melibatkan pencurian kekayaan intelektual itu sendiri;
e. Korupsi kegiatan perbankan dan keuangan internasional;
f. Penyelundupan manusia;
g. Kejahatan siber dan perang informasi;
h. Kejahatan maritim;
i. Pencucian uang;

[75] Roderic Broadhurst dan Peter Grabosky, *Cybercrime The Challenge in Asia*, Hongkong University Press, Hongkong, 2005, hlm, 214.
[76] John Broome, 2000, *Transnational Crime in The Twenty-First Century*, Transnational Crime Conference, Canberra, hlm. 3-4.

j. Terorisme nasional;
k. Keterlibatan *organized crime.*

2. *The Group of Eight* (G8)

The Group of Eight atau dikenal G8 adalah kelompok negara-negara industri yang terdiri dari: Kanada, Jerman, Perancis, Italy, Jepang, Inggris, Amerika Serikat, dan Rusia.[77] G8 dalam *Meeting of Justice and Interior Ministers of The Eight* yang diselenggarakan pada tanggal 9-10 desember 1997 yang membahas dua tugas penting yaitu meningkatkan kemampuan untuk melakukan penyidikan dan penuntutan kejahatan teknologi tinggi (*high tech crime*) dan memperkuat instrumen hukum internasional untuk ekstradisi dan bantuan timbal balik untuk menjamin bahwa tidak ada pelaku tindak pidana yang memperoleh tempat aman di dunia ini. Menurut G8 setidaknya ada dua bentuk ancaman terhadap keamanan umum yang lebih besar dari yang pernah ada, yaitu:[78]

a. *Sophisticated criminals are targeting computer and telecommunications system to obtain or alter valuable information without authority and may attempt to disrupt critical commercial adn public systems*. (para pelaku kejahatan yang canggih menjadikan komputer dan sistem

[77] G8 berakar dari krisis minyak 1973 dan resensi dunia yang terjadi selanjutnya. Masalah-masalah ini membuat Amrerika Serikat mendirikan kelompok bernama Library Group, sebuah perkumpulan para pejabat keuangan senior dari Amerika Serikat, Eropa, Dan Jepang, untuk mediskusikan masalah ekonomi. Pada tahun 1975 Presiden Prancis mengundang para kepala negara (enam negara) demokratis besar yang maju ke pertemuan G6 yang pertama di Rambouillet dan menawarkan ide untuk adanya pertemuan tetap. Para Negara yang setuju untuk adanya pertemuan tetap tersebut mendirikan kelompok G6 yang terdiri dari Prancis, Jerman, Italy, Jepang, Amerika Serikat, dan Britannia Raya. Pada pertemuan kedua di Puerto Rico, G6 menjadi G7 dengan masuknya Kanada. Setelah berakhirnya perang dingin Rusia mulai bertemu dengan G7 setelah pertemuan pertama. Sejak tahun 1997-2014 Rusia bergabung dengan G8 akan tetapi, setelah bergabungnya Krimea ke Rusia, keanggotaan Rusia dalam kelompok tersebut ditangguhkan, T Mhd Aulia Fitra, *Op.cit*., hlm. 31.

[78] *Ibid*., hlm. 32.

telekomunikasi sebagai target untuk memperoleh atau mengalihkan informasi yang berharga tanpa izin dan mencoba untuk mengganggu sistem-sistem perdagangan penting dan sistem-sistem publik lainnya)

b. *Criminals, including members of organized crime groups and terorists, are using these new technologies to facilitate traditional offenses*. (Para pelaku kejahatan, termasuk anggota dari kelompok penjahat terorganisir dan para teroris, menggunakan teknologi baru ini sebagai alat untuk melakukan kejahatan tradisional)

3. *Council of Europe (COE)*

Council of Europe merupakan organisasi supranasional yang berada di Eropa. Pada tahun 1985 dibentuk sebuah komite ahli yaitu *Europe Committee on Crime Problems* untuk mempertimbangkan berbagai masalah hukum yang ditimbulkan oleh kejahatan komputer. Salah satu laporan yang dihasilkan pada September 1989 tersebut ialah bentuk-bentuk kejahatan kejahatan siber yang harus diatur dalam hukum nasional berupa:[79]

a. *Computer fraud*
Memasukkan, mengubah, menghapus atau menahan data komputer atau program komputer atau gangguan lainnya dalam pengolahan data yang memengaruhi hasil dari pengolahan data sehingga menimbulkan hilangnya nilai ekonomis atau kepemilikan properti pada orang lain dengan maksud memperoleh keuntungan ekonomi secara melawan hukum untuk diri sendiri atau orang lain.

b. *Computer forgery*
Memasukkan, mengubah, menghapus atau menahan data komputer atau program komputer atau gangguan lainnya dalam pengolahan data dengan cara atau dalam kondisi tertentu sebagaimana digambarkan dalam hukum

[79] Convention on Cybrecrime di buat di Budapest, Hungaria yang digagas oleh Uni Eropa yang berjumlah 35 Negara Eropa, ditambah dengan Australia, Republic Dominician, Jepang dan Amerika Serikat. Konvensi ini mengatur kebijakan kriminal dan merumuskan tindak pidana untuk meningkatkan kerja sama antar Negara dalam menangani cybercrime, Sigid Suseno, *Op.Cit*., hlm. 114

nasionalnya, perbuatan tersebut dapat termasuk tindak pemalsuan jika hal itu dilakukan berkenaan dengan objek tradisional dari tindak pidana tersebut

c. *Damage to computer data or computer programs*
   Menghapus, merusak, memperburuk atau menahan data komputer atau program komputer tanpa hak.
d. *Computer sabotage*
   Memasukkan, mengubah, menghapus atau menahan data komputer atau program komputer atau gangguan lainnya dalam sistem computer dengan maksud untuk mengganggu fungsi sistem komputer atau sistem telekomunikasi.
e. *Unauthorized access*
   Mengakses sistem komputer atau jaringan komputer secara tanpa hak dengan melanggar sistem pengamanan.
f. *Unauthorized interception*
   Melakukan intersepsi secara tanpa hak dengan cara-cara teknis, dengan mengumumkan dari dan dalam sistem komputer atau jaringan computer
g. *Unauthorized reproduction of a protected computer program*
   Menggandakan, mendistribusikan atau mengumumkan program computer yang diliindungi hukum kepada umum secara tanpa hak
h. *Unauthorized reproduction of a topography*
   Menggandakan topografi yang dilindungi hukum secara tanpa hak dari produk semikonduktor atau mengeksploitasi secara komersial atau memasukkan topografi atau produk semi konduktor yang dihasilkan dari penggunaan topogarafi dengan tujuan untuk itu dilakukan tanpa hak.

Pada April 1997, komite menyusun instrumen Internasional yang komprehensif tentang tindak pidana siber yaitu *Convention on Cybercrime* dan selesai pada tahun 2001. Komite melaksanakan tugas tersebut selama 4 tahun dengan melalui 27 draf konvensi sebelum sampai pada *Final Draft Convention on Cybercrime* yang diterima oleh *European Committee on Crime Problems* dalam rapat pleno Juni 2001. *Convention on Cybercrime* telah diterima dan terbuka untuk ditandatangani pada 23 November 2001 di Budapest,

Hungaria. *Convention on Cybercrime* 2001 terbuka untuk ditandatangani oleh negara selain anggota *Council of Europe* yang ikut berpartisipasi dalam pembahasan konvensi tersebut seperti Kanada, Jepang, Afrika Selatan, dan Amerika Serikat. Namun demikian untuk masa yang akan datang, dengan persetujuan secara bulat dari negara-negara peserta konvensi, Komite Menteri *Council of Europe* dapat mengundang negara-negara yang bukan anggota *Council of Europe* untuk mengaksesi konvensi ini.[80]

4. *Convention on Cybercrime*

Convention on Cybercrime secara umum telah dianggap sebagai salah satu peraturan hukum internasional yang mengatur mengenai kejahatan siber. *Convention on Cybercrime* merupakan aturan regional untuk negara anggota *Council of Europe*. Konvensi ini telah dibuka untuk ditandatangani sejak 23 November 2001 namun mulai berlaku pada tahun 2004. Hingga tahun 2014, terdapat sebanyak empat puluh lima negara yang menandatangani konvensi tersebut, Monako menjadi negara anggota *Council of Europe* terbaru yang menandatangani konvensi tersebut yaitu pada 2 Mei 2013. Dari sebanyak empat puluh lima negara anggota yang menandatangani konvensi tersebut, sebanyak tiga puluh enam negara yang telah

[80] T Mhd Aulia Fitra, Op.cit., hlm. 35.

meratifikasinya dan terdapat dua negara anggota yang tidak menandatangani konvensi tersebut yaitu Rusia dan San Marino.[81]

Selain negara anggota *Council of Europe*, terdapat juga beberapa negara diluar negara anggota yang menandatangani konvensi tersebut, yaitu Kanada, Jepang, Afrika Selatan, dan Amerika Serikat. Jepang dan Amerika telah melakukan ratifikasi terhadap konvensi tersebut, sedangkan Australia, Dominika, dan Mauritius telah melakukan aksesi terhadap konvensi dan negara-negara tersebut telah meratifikasi konvensi. Argentina, Bostwana, Mesir, Nigeria, Pakistan dan Filipina mengadopsi ketentuan dalam konvensi tanpa mengaksesi *Convention on Cybercrime*.[82]

Melihat dari banyaknya jumlah negara yang menandatangani dan bahkan yang meratifikasi konvensi tersebut, dapat dikatakan bahwa untuk saat ini konvensi tersebut merupakan peraturan internasional yang paling banyak dijadikan acuan utama dalam pembentukan peraturan perundang-undangan mengenai kejahatan siber. Indonesia sendiri mengadopsinya dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik *Jo.* Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dengan sebagian besar materinya diterapkan.

5. *Pedoman International Telecommunication Union*

[81] Josua Sitompul, 2012, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*, Tatanusa, Jakarta, hlm. 106

[82] *Ibid*., hlm. 107.

International Telecommunication Union (ITU) pada tahun 2009 telah mengeluarkan dokumen *Understanding Cybercrime: A Guide for Developing Countries.*[83] Pedoman ini memberikan gambaran mengenai karakteristik kejahatan siber kepada negara-negara di dunia sehingga tiap negara dapat mengetahui perbuatan-perbuatan apa saja yang dapat dikriminalisasi dalam perundang-undangan. Pedoman ini mengembangkan pengaturan-pengaturan yang telah dimuat dalam *Convention on Cybercrime*.

6. Upaya *Association of South East Asian Nation* (ASEAN)

Negara-negara ASEAN juga telah melakukan pembahasan mengenai pentingnya masalah kejahatan siber terutama mengenai tindak pidana terorisme, penyelundupan senjata, ataupun pemalsuan dokumen perjalanan. Pada pertemuan ASEAN *Inter-Sessional Support Group on Confidence Building Measures* di Yangon, Myanmar tanggal 11-14 April 2004, negara-negara peserta mengakui bahwa kejahatan siber merupakan salah satu isu non-tradisional yang menimbulkan tantangan serius sehingga membutuhkan kerja sama dan dukungan antar negara anggota. Untuk menangani tindak pidana siber dibutuhkan pertukaran informasi dan data intelijen antar negara anggota serta pengembangan aparat penegak hukum. Berdasarkan hasil dari Konferensi Kepala-Kepala Kepolisian Negara-Negara ASEAN, peserta konferensi menyepakati agar negara-negara

[83] *Ibid*., hlm. 121

anggota tetap mendukung pembentukan peraturan perundang-undangan yang mengatur kejahatan siber di negara masing-masing.

Berdasarkan uraian di atas, maka dapat dikatakan bahwa serangan siber yang menggunakan virus *Ransomware WannaCry* merupakan salah satu bentuk dari kejahatan siber. Dikatakan sebagai salah satu bentuk kejahatan siber, karena serangan siber menggunakan virus *Ransomware WannaCry* ini memenuhi kriteria atau indikator yang termasuk dalam jenis-jenis kejahatan siber sebagaimana yang diatur dalam *Convention on Cybercrime* (COC), yakni:

1. Akses ilegal (*illegal access*)
2. Gangguan terhadap data (*data interference*)
3. Gangguan terhadap sistem (*system interference*)

Dikategorikannya serangan siber menggunakan virus *Ransomware WannaCry* ke dalam tindakan akses ilegal, gangguan terhadap data, dan gangguan terhadap sistem tidak lepas dari tujuan dan akibat yang ditimbulkan oleh virus itu sendiri, yakni *Ransomware WannaCry* digunakan sebagai alat untuk mengakses dan merampas data milik orang lain dari komputernya yang bersifat pribadi dan dapat mematikan sistem komputer korbannya sehingga tidak dapat diakses selama virus tersebut masih menginfeksi.

Dari segi aturan, secara internasional telah ada peraturan maupun upaya-upaya dari PBB, Uni Eropa, dan ASEAN dalam menghadapi kejahatan siber dan juga telah ada pedoman yang telah diberikan ITU

sebagai pedoman negara-negara di dunia dalam menyikapi kejahatan siber. *Convention on Cybercrime* sebagai aturan yang telah ditandatangani banyak negara dan bahkan telah diratifikasi oleh beberapa negara diluar negara anggota *Council of Europe* menjadikan konvensi ini sebagai acuan negara-negara di dunia dalam membuat instrumen hukum yang mengatur mengenai kejahatan siber dalam sistem hukum nasional mereka. Meskipun demikian, dalam melacak dan menindak pelaku kejahatan siber menggunakan virus *Ransomware WannaCry* dibutuhkan kerjasama antar negara mengingat virus ini terjadi lintas negara dan setiap negara memiliki kedaulatan dan sistem hukum yang harus dihormati oleh negara lainnya.

BAB III

TINJAUAN PUSTAKA DAN ANALISIS PERMASALAHAN KEDUA

A. Kejahatan Siber Dalam Undang-Undang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan payung hukum dari kejahatan siber dalam sistem hukum nasional. UU ITE adalah undang-undang yang dibuat oleh pemerintah Indonesia yang mengatur dua muatan besar, yaitu kejahatan siber dan transaksi elektronik. Materi UU ITE merupakan implementasi dari beberapa prinsip ketentuan internasional, yaitu *Convention on Cybercrime*, *UNCITRAL Model Law on Electronic Commerce, UNCITRAL Model Law on Electronic Signature, EU Directives on Electronic*