

SKRIPSI
PENANGGULANGAN KEJAHATAN CYBER CRIME YANG DI
LAKUKAN OLEH HACKER DALAM TINJAUAN HUKUM
KEJAHATAN INTERNASIONAL
(STUDI KASUS CYBER CRIME POLDA SULSEL)



Syabilah Yuka Kawandoda

Stb 040 2017 0376

FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA
MAKASSAR
2022

HALAMAN JUDUL

**PENANGGULANGAN KEJAHATAN CYBER CRIME
YANG DILAKUKAN OLEH HACKER DALAM
TINJAUAN HUKUM KEJAHATAN INTERNASIONAL**

Diajukan dan Disusun

Oleh

Syabilah Yuka Kawandoda

Skripsi

**Diajukan Sebagai Tugas Akhir Dalam Rangka
Penyelesaian Studi Sarjana Pada Bagian Hukum
Pidana**

PADA

**FAKULTAS HUKUM
UNIVERSITAS MUSLIM INDONESIA**

MAKASSAR

2022

PERSETUJUAN PEMBIMBING

Diterangkan bahwa Proposal di bawah ini :

Judul Skripsi : **Penanggulangan Kejahatan Cyber Crime Yang Di Lakukan Oleh Hacker Dalam Tinjauan Hukum Kejahatan Internasional (Studi Kasus Cyber Crime Polda SulSel)**

Nama Mahasiswa : **Syabilah Yuka Kawandoda**

No. Stambuk : **04020170376**

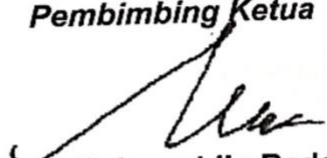
Program Studi : **Ilmu Hukum**

Bagian : **Hukum Pidana**

Dasar Penetapan : **SK.DEKAN NO.0152/H.05/FH-UMI/II/2021**

Telah di periksa dan di setujui untuk diajukan dalam ujian tutup.

Pembimbing Ketua


Dr. H. Baharuddin Badaru ,SH.,MH.

Pembimin Anggota


Dr. Dachran S. Busthami ,SH.,MH.

**Mengetahui,
Ketua Bagian Hukum Pidana**

Prof. Dr. Hj. Mulyati Pawennei, S.H.,M.H.



PERSETUJUAN UJIAN SKRIPSI

Pimpinan Fakultas Hukum Universitas Muslim Indonesia

Persetujuan untuk mengikuti ujian Skripsi kepada

Nama Mahasiswa : **Syabilah Yuka Kawandoda**

No. Stambuk : **04020170376**

Program Studi : **Ilmu hukum**

Bagian : **Hukum Pidana**

Judul Skripsi : **Penanggulangan Kejahatan Cyber Crime
Yang Dilakukan Oleh Hacker Dalam Tinjauan
Hukum Kejahatan Internasional(Studi Kasus
Cyber Crime Polda Sulsel)**

Dasar Penetapan : **SK. DEKAN NO. 0153/H.05/FH-UMI/II/2021**

Telah di periksa dan di setujui untuk diajukan dalam ujian skripsi sebagai
ujian akhir program studi.

Makassar,..... 2022

Dekan Fakultas Hukum

Universitas Muslim Indonesia



Prof. Dr. H. La Ode Husen, S.H., M.H.,
NIPs 104860192

HALAMAN PENGESAHAN

Diterangkan bahwa skripsi tersebut di bawah ini :

Nama Mahasiswa : Syabilah Yuka Kawandoda

Nim : 040 2017 0376

Bagian : Hukum Pidana

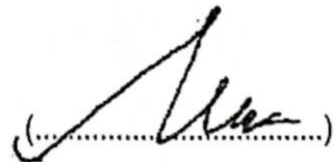
Dasar Penetapan : NO.0152/H.05/FH-UMI/II/2021

Judul Skripsi/Penelitian : **Penanggulangan Kejahatan Cyber Crime Yang di Lakukan oleh Hacker dalam Tinjauan Hukum Kejahatan Internasional (Study Kasus Cyber Cryme Polda SulSel)**

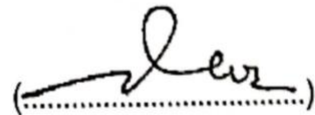
Telah dipertahankan dihadapan dan diterima oleh panitia ujian skripsi

Disahkan Oleh :

Dr.H. Baharuddin Badaru,S.H.,M.H.



Dr. Dachran S.Busthami,S.H.,M.H.



Prof. Dr. H. Hambali Thalib,SH.,MH.



Rizki Ramadani,SH.,MH.



PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini:

Nama Mahasiswa : Syabilah Yuka Kawandoda

Nim : 040 2017 0376

Bagian : Hukum Pidana

Judul Skripsi/Penelitian : Penanggulangan Kejahatan Cyber Crime Yang di Lakukan oleh Hacker dalam Tinjauan Hukum Kejahatan Internasional (Study Kasus Cyber Cryme Polda SulSel)

Menyatakan dengan sebenarnya bahwa skripsi saya ini benar merupakan hasil karya sendiri , bukan merupakan hasil plagiasi terhadap karya ilmiah orang lain. Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan dari skripsi merupakan hasil plagiasi maka saya bersedia menerima sanksi karena perbuatan tersebut.

Makassar, Oktober 2022

Yang menyatakan,



Syabilah Yuka Kawandoda

KATA PENGANTAR

Puji dan syukur kehadiran Allah SWT, karena dengan rahmat, taufik dan inayah-Nya sehingga penyusunan Skripsi ini dengan judul **“Penanggulangan Kejahatan Cyber Crime Yang Dilakukan Oleh Hacker Dalam Tinjauan Hukum Kejahatan Internasional (Studi Kasus Cyber Crime Polda Sulsel)”** dapat dirampungkan sesuai dengan waktu yang direncanakan. Tak lupa penulis kirimkan salawat dan salam kepada Nabi Muhammad SAW sebagai teladan bagi seluruh umat manusia.

Disadari bahwa Skripsi ini kurang sempurna, hal ini disebabkan karena keterbatasan kemampuan yang ada pada penulis. Oleh karena itu, kritik, saran dan koreksi untuk perbaikan dan penyempurnaan sangat penulis harapkan.

Pada kesempatan ini, perkenankanlah penulis menyampaikan rasa terima kasih diiringi do'a kepada Allah SWT., kepada Kedua orang tua penulis Ayahanda **Yerri Kawandoda** dan Ibunda **Darmakiyah** yang telah mendidik, membesarkan dan membimbing serta doa yang tulus. Selanjutnya diucapkan terima kasih kepada:

1. **Bapak Prof. Dr. Basri Modding, SE., M.Si.**, selaku Rektor Universitas Muslim Indonesia;

2. **Bapak Prof. Dr. H. La Ode Husen, S.H., M.H.**, selaku Dekan Fakultas Hukum Universitas Muslim Indonesia;
3. **Ibu Prof. Dr. Hj. Muliati Pawennei, S.H., M.H.**, selaku Ketua Bagian Hukum Pidana Fakultas Hukum Universitas Muslim Indonesia; yang telah memberikan izin, kesempatan dan fasilitas kepada Penulis selama mengikuti pendidikan Program Sarjana;
4. **Bapak Dr. H. Baharuddin Badaru ,SH.,MH.** Dan **Bapak Dr. Dachran S.Busthami ,SH.,MH.** Selaku Ketua dan Anggota Pembimbing yang memberikan bimbingan, dengan penuh keseriusan, kecermatan dan kebijakan dalam memberi petunjuk-petunjuk perihal prinsip penulis karya ilmiah kepada penulis;
5. **Bapak Prof. Dr. H. Hambali Thalib, S.H., M.H.**, dan **Bapak Rizki Ramadani, S.H., M.H.**, Selaku penilai yang memberikan masukan dan saran pada ujian Seminar Proposal sampai Ujian Skripsi;
6. **Bapak Widoni**, Selaku Kepala Ditreskrimsus Kepolisian Daerah Sulawesi Selatan yang memberikan izin untuk melakukan penelitian di Kepolisian Daerah Sulawesi Selatan.

Kepada seluruh sahabat-sahabat yang tak sempat Penulis sebutkan satu persatu dalam tulisan ini, Penulis ucapkan terima kasih atas bantuan dan kebersamaannya.

Akhirnya Penulis mengharap semoga dengan hadirnya Skripsi ini dapat bermanfaat bagi pengembangan ilmu dan teknologi.

Semoga Allah SWT, senantiasa memberkati dan merahmati segala aktivitas keseharian sebagai suatu ibadah disisi-Nya. Aamiin.

Makassar,... 2022

Penulis

Syabilah Yuka Kawandoda

ABSTRAK

Syabilah Yuka kawandoda, 04020170376 : "*Penanggulangan Kejahatan Cyber Crime Yang Dilakukan Oleh Hacker Dalam Tinjauan Hukum Kejahatan Internasional (Studi Kasus Cyber Crime Polda Sulsel)*" Di bawah bimbingan (Baharuddin Badaru) sebagai ketua pembimbing dan (Dachran S.Busthami) sebagai Anggota pembimbing.

Penelitian ini bertujuan untuk mengetahui dan menganalisis penegakan hukum terhadap Kejahatan Cyber Crime oleh penyidik Polda Sulsel , serta, mengetahui dan menganalisis hambatan penyidik dalam penanganan kasus Cyber Crime yang dilakukan oleh Hacker di Polda Sulawesi Selatan.

Penelitian ini menggunakan Metode Penelitian Hukum (Legal Research) dengan tipe penelitian empiris yaitu melakukan penelitian kepustakaan dengan meneliti dan pengumpulan bahan-bahan kepustakaan yang khususnya berkaitan dengan peraturan perundang- undangan dan buku-buku yang berkaitan tentang hukum, serta penelitian lapangan yang dilakukan dengan pengamatan observasi dan wawancara langsung dengan objek yang berkaitan.

Hasil penelitian ini menunjukkan bahwa kejahatan cyber crime yang dilakukan oleh hacker rata – rata melakukan kejahatan dengan tehnik phishing atau mengirim link kepada korban dengan bertujuan mengambil data milik korban baik melalui e-mail atau pun facebook korban. Media sosial yang sering di akses masyarakat : facebook, whatsapp, Instagram, dan lain-lain. Bentuk informasi yang di dapat melalui media social tersebut adalah data pribadi ataupun informasi umum, biodata, foto, video, informasi kartu kredit (CC), dan lain sebagainya. UU No. 19 Tahun 2016. Pasal 30 ayat (1) UU ITE yang berbunyi "*Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun*".

Kata Kunci : Analisis Hukum, Kepolisian, Cyber Crime, Hacker

DAFTAR ISI

Sampul	i
Persetujuan Pembimbing	ii
Persetujuan Ujian Skripsi	iii
Kata Pengantar	iv
Abstrak	vii
Daftar Isi	viii
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	7
C. Tujuan dan Manfaat Penelitian	8
BAB II TINJAUAN PUSTAKA	9
A. Definisi Hukum Kejahatan Internasional	9
B. Karakteristik Tindak Pidana Internasional	12
C. <i>Cyberspace, Cyber Law</i> dan <i>Cybercrime</i>	16
D. Modus Operandi dan Jenis Serangan Hacker	28
a. Physically Hacking	28
b. <i>Logically Hacking</i>	29
E. Definisi dan Aspek-Aspek Pertahanan keamanan.....	33
BAB III METODOLOGI PENELITIAN	36
A. Lokasi Penelitian	36
B. Jenis Data	36
C. <i>Teknik Pengumpulan</i>	37

D. Analisis Data	37
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	38
A. Penanggulangan Kejahatan Cyber Dalam Tinjauan Hukum Kejahatan Internasional	38
B. Efek yang ditimbulkan oleh serangan <i>Hacker</i> dan implikasinya terhadap Pertahanan dan Keamanan Negara	44
1. Penguasa	~~38~~
2. Penghancur	~~44~~
BAB V PENUTUP	46
Kesimpulan	46
Saran	46
DAFTAR PUSTAKA	47

BAB I

PENDAHULUAN

A. Latar Belakang

Revolusi teknologi komputer menjadi media informasi dan komunikasi global yang saat ini menjadi pembicaraan hangat dalam masyarakat kelas menengah negeri ini menjadikan Internet menjadi suatu kebutuhan yang tidak bisa ditawar-tawar lagi. Bila dikaitkan dengan sistem komputer, faktor manusia (*Brainware*) sangat menentukan akan perkembangan teknologi komputer.

Beberapa ahli telah mencoba mendefenisikan pengertian dari penyalahgunaan komputer, baik dalam suatu Undang-undang ataupun dalam suatu rancangan Undang-undang sehingga muncul berbagai macam definisi mengenai penyalahgunaan komputer atau tindak pidana yang menggunakan sarana komputer.¹

Kemajuan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet. Kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (*real*) ke

¹ Edmon Makarim,SH,S.Kom,,LL.M Kompilasi Hukum Telematika PT. Raja Grafindo Persada; Jakarta, 2003 Hal 5-6

realitas baru yang bersifat maya (*Virtual*).

Realitas yang kedua ini biasa dikaitkan dengan internet dan *cyber space*. Perkembangan internet yang semakin hari semakin meningkat, baik perangkat maupun penggunaannya, membawa dampak positif atau pun negatif. Untuk yang bersifat positif kita pantas bersyukur, karena banyak manfaat dan kemudahan yang kita dapatkan dari teknologi ini. Tetapi tidak dapat dipungkiri bahwa teknologi internet membawa dampak negatif yang tidak kalah banyaknya dari manfaatnya.

Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan menjadi lebih canggih melalui penggunaan media komputer secara *online* dengan resiko tertangkap yang sangat kecil. Dari paparan di atas tentang realitas efek positif maupun negatif komputer, tulisan ini akan memfokuskan pada *Cyber Crime*, contoh kasus dan tinjauan hukumnya menurut hukum kejahatan Internasional.

Cyber Crime adalah kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber* atau di dunia maya yaitu dengan melalui internet. Tidak semua *cybercrime* dapat langsung dikategorikan sebagai kejahatan dalam artian yang sesungguhnya. Ada pula jenis kejahatan yang masuk dalam “wilayah abu-abu”, salah satunya adalah *probing* atau *portscanning*. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak - banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, port- port (kanal- kanal komputer) yang ada, baik yang terbuka maupun tertutup, dan sebagainya.

Berbicara masalah *cyber crime* 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 dunia maya (*cyber crime*) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat. Untuk lebih mendalam ada beberapa pendapat di bawah ini tentang apa yang dimaksud dengan *cyber crime*? Di antaranya adalah menurut Kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan criminal dan / atau criminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital².

Kalau dianalogikan, kegiatan ini mirip dengan pencuri yang melakukan survey terlebih dahulu terhadap sasaran yang dituju. Di titik ini pelakunya tidak melakukan tindakan apapun terhadap sistem yang diintainya, namun data yang ia dapatkan akan sangat bermanfaat untuk melakukan aksi sesungguhnya³.

Berkembangnya kejahatan Internasional yang hidup ditengah- tengah masyarakat ,mendorong para pakar hukum internasional untuk memberikan perhatian yang serius terhadap perkembangan kejahatan internasional tersebut dalam bentuk penelitian-penelitian.

² Abdul Wahid dan Mohammad Labib, *Kejahatan*., hlm. 40

³ Cyber Crime « [X-Database].htm. Diakses pada tanggal 22 November 26, 2010 pukul:13.47

Hasil dari penelitian para pakar tersebut menghasilkan sejumlah teori atau kaidah baru yang memberikan tambahan pemahaman kepada masyarakat akan kejahatan internasional.

Penelitian tersebut telah memberikan hasil yang tidak sedikit, hal ini dibuktikan dengan hadirnya sejumlah karya tulis yang dapat dijadikan sebagai referensi dalam pengembangan keilmuan salah satu cabang kajian dari hukum internasional ini.⁴

Dalam karya-karya tersebut para pakar hukum internasional mencoba mengemukakan kehadiran hukum kejahatan internasional ditengah masyarakat internasional. Sebagai contoh pendapat yang dikemukakan oleh Bassiouni yang menyatakan sebagai berikut: ⁵

“International criminal law becoming increasingly relevant to our contemporary world, and it will surely continue become an ever more important legal discipline. Present and future generations of student of the law and all fields such as political science and criminology, will need to learn more about subject deals with the problem of international and transnational which are constantly increasing in number, intensity and threat to the peace and stability of the world order and security and safety of individuals all over the world. These danger come from states, individuals and groups from every corner of the globe.

Selain pendapat yang dikemukakan oleh Bassiouni, Muller R. Wise juga mengemukakan pendapatnya yang berkenaan hadirnya *International Criminal Law* atau Hukum Kejahatan Internasional dimana beliau mengatakan bahwa:⁶

⁴ Romli Atmasasmita, *Pengantar Hukum Pidana Internasional*, Refika Aditama; Bandung, 2000 hal. 5

⁵ Bassiouni *International Criminal Law Vol.iii Enforcement*, Transnational Publisher; New York, 1987 hal xiii, dikutip dari Romli Atmasasmita, *Pengantar Hukum Pidana Internasional*, Refika Aditama; Bandung, 2000 hal.6

⁶ Ibid hal.6-7

“ There has in fact emerged a body of principles which justifiable maybe entitled “International Criminal Law”. This is a term quiet familiar to continental lawyers who in tradition code lawyer have long been busily engaged in assembling the members of the body. Often before there was any “positive” law in point. In anglo American Law we have become active at a somewhere laterstage in the evolution of “International Criminal Law”.

Pendapat Muller R. Wise, menunjukkan fakta dari kesatuan asas - asas yang dapat dipertanggung jawabkan sebagai “Hukum Kejahatan Internasional”. Dari dua pendapat pakar hukum internasional tersebut, khususnya pendapat yang dikemukakan oleh Muller R. Wise, dapat ditarik kesimpulan bahwa mulai dari awal abad Ke-20 hukum kejahatan internasional yang merupakan cabang dari hukum internasional baru berkembang di belahan bumi yang menganut sistem hukum *anglo saxon*.

Kenyataan ini juga yang menyebabkan terjadinya Revolusi (1947) yang menghendaki dilaksanakannya pembentukan suatu panitia kodifikasi hukum internasional *The Committee on Codification of International Criminal Law* yang bertugas merumuskan prinsip-prinsip hukum internasional yang telah diakui dalam : *The Charter And Tribunal Of Nurenberg Trial* 1945) sebagai sebuah pengakuan internasional terhadap cabang baru dalam hukum internasional.

Kejahatan *Cyber* atau *Cybercrime* pada dasarnya yang merupakan imbas dari kemajuan teknologi yang telah mengubah kebiasaan masyarakat yang pada awalnya bersifat konvensional menjadi sebuah kebiasaan yang lebih bersifat modern atau dapat disebut *high technology society*. Perubahan kebiasaan ini telah menghasilkan suatu kejahatan dengan penggunaan alat elektronik sebagai media kejahatan.

Faktor utama yang menyebabkan peralihan kebiasaan tersebut adalah adanya perkembangan teknologi informasi yang berpadu dengan media komunikasi berteknologi komputer, yang kemudian menghasilkan suatu piranti baru yaitu Internet⁷.

Dengan munculnya internet telah menimbulkan suatu pola interaksi baru dalam kehidupan bermasyarakat, yang pada awalnya lebih bersifat nyata (*real*) berubah menjadi pola interaksi masyarakat yang lebih cenderung bersifat virtual (*cybernetics*).

Perkembangan internet yang semakin meningkat tentu saja memiliki implikasi terhadap lahirnya komunitas baru dalam masyarakat yang melakukan aktivitasnya dalam dunia virtual yang menimbulkan ketakjuban walaupun kadang menimbulkan rasa takut. Di sisi positif dalam artian lain “sisi terang”, masyarakat dapat menemukan komunitas IT seperti *programmer, teknisi, dan blogger*. Sedangkan disisi lain masyarakat melihat komunitas ini yang melakukan aktivitas - aktivitas yang mengakibatkan kerusakan dan kerugian yang tidak sedikit.

⁷ Abdul Wahid dan Muhammad Labib, *Kejahatan Mayantara (Cybercrime)*, PT Refika Aditama, Jakarta 2005, hal 103

Banyak juga masyarakat yang memandang komunitas hacker sebagai komunitas yang berimplikasi negatif, padahal pandangan terhadap komunitas *hacker* tersebut adalah pandangan yang sangat keliru. Dalam sejarah banyak tercatat kesalahan - kesalahan yang mengakibatkan buruknya pandangan masyarakat awam terhadap komunitas *hacker*, baik yang terjadi dalam skala nasional, regional maupun internasional.

Kesalahpahaman tersebut akibat ketidakpahaman masyarakat awam dalam membedakan *white hat hacker (hacker)*, *black hat hacker (craker)*, dan *grey hat hacker*. Sudah banyak contoh kasus yang terjadi bahkan sejak 21 tahun lalu dan jauh sebelumnya, sederetan kasus tersebut menunjukkan aktivitas *hacker* dan kelompok IT lainnya.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas maka untuk memfokuskan penulisan proposal ini maka rumusan masalah yang akan dibahas adalah

1. Bagaimanakah bentuk kejahatan *Cyber* yang dilakukan oleh *Hacker* dalam tinjauan hukum kejahatan internasional ?
2. Bagaimanakah efek yang ditimbulkan oleh serangan Hacker dan implikasinya terhadap pertahanan dan keamanan Negara ?

C. Tujuan dan Manfaat Penelitian

Tujuan Penelitian

1. Menemukan modus operandi dari kejahatan *Cyber* yang dilakukan oleh *Hacker* dalam *Cyberspace* sebagai sebuah bentuk kejahatan baru yang lebih bersifat modern dan memiliki efek yang sangat besar terhadap privasi masyarakat dan keamanan suatu negara sehingga menjadikan kejahatan ini sebagai kejahatan yang bersifat Internasional.
2. Memberikan suatu jalan keluar terhadap keterbatasan – keterbatasan yang dialami oleh masyarakat dan negara dalam mmenanggulangi kejahatan *Cyber* yang dilakukan oleh *Hacker*

Manfaat Penelitian

1. Diharapkan dengan penelitian ini dapat meluruskan paradigma masyarakat terhadap komunitas *Hacker*
2. Menambah khasanah pengetahuan masyarakat terhadap komunitas yang hadir dalam dunia virtual (*cyber*) melalui ciri khas dan faktor yang dapat mengganggu privasi masyarakat banyak dan keamanan suatu negara sehingga kejahatan ini dapat digolongkan sebagai suatu kejahatan internasional.
3. Menemukan suatu gagasan demi terciptanya suatu metode penanggulangan kejahatan dunia virtual (*cyber*) yang dilakukan oleh *hacker*.

BAB II

TINJAUAN PUSTAKA

A. Definisi Hukum Kejahatan Internasional

Sampai saat ini belum ada suatu ketentuan di dalam hukum internasional, baik dalam perjanjian – perjanjian internasional maupun dalam kebiasaan internasional yang melakukan penetapan atas istilah “*International Crimes*”. Perdebatan mengenai peristilahan ini disebabkan karena dua hal, yang pertama adalah permasalahan istilah “*International Crimes*” yang belum dapat diterima oleh para pakar sebagai istilah yang tepat dalam menggambarkan tindakan yang dapat dikategorikan dalam kejahatan internasional.

Selain itu pelaku dari kejahatan internasional sendiri bukan hanya individu atau kelompok tertentu melainkan juga sebuah Negara atau institusi resmi (seperti dalam beberapa kasus kejahatan internasional dalam Nurenberg Trial, Yugoslavia (ICTY), Sudan (Presiden Omar Al-Bashir) dan beberapa negara lainnya dalam proses penyelesaian melibatkan sejumlah petinggi negara seperti “Presiden”.

Selain itu masih terjadi pertentangan antara pakar – pakar hukum internasional mengenai perbedaan antara *international deliquencies* dengan *international crime* . Dalam buku Oppenheim edisi kedelapan yang diedit oleh H. Lauterpacth mengatakan mengenai perbedaan yang terdapat pada *international deliquencies* dan *international crime* yang terkhusus pada tanggung jawab yang harus dilakukan oleh negara sebagai sebuah hakikat yang timbul dari tindakan tersebut.

Pendapat tersebut dapat dijadikan sebagai dasar untuk memberikan kejelasan bahwa "*international deliquencies*" tidak dapat dikategorikan sebagai suatu kejahatan, karena negara dianggap melakukan tindakan delikuen dan tindakan delikuen tersebut tidak bisa dijatuhi hukuman dan seandainya pertanggungjawaban dapat dipaksakan, maka pertanggungjawaban tersebut hanyalah sebatas untuk memperbaiki tindakan yang tidak benar.

Sejalan dengan sifat hukum internasional yang mengatur hubungan antar negara yang berdaulat dan bukan sebuah perangkat hukum diatas semua negara. Negara – negara berdaulat telah mengesampingkan kemungkinan penjatuhan pidana atas negara karena melakukan tindakan yang tidak benar (*delinquency*)⁸.

Pada awalnya tindakan yang dapat dikategorikan sebagai kejahatan internasional atau *international crime* hanya terdapat empat jenis tindak kejahatan yakni *war crimes* atau kejahatan perang, *genocide* atau genosida, *crimes against humanity* atau kejahatan terhadap kemanusiaan, dan *aggression* atau agresi yang pada akhirnya berkembang menjadi 22 jenis kejahatan.

Definisi 22 jenis kejahatan tersebut adalah 22 jenis kejahatan yang dikemukakan oleh Bassiouni dimana kejahatan tersebut antara lain *Aggression, War Crimes, Unlawful Use Of Weapon, Crime Againts Humanity, Genocide, Racial Discrimination and Apartheid, Slavery and Related Crime, Torture, Unlawful Human Experimentation, Piracy, Aircraft*

⁸ Schwasenberger, *The Problem Of An International Criminal Law*, Steven and Sons, LTD ; London, 1950, hal. 13-14, dikutip dari Romli Atmasasmita, Pengantar Hukum Pidana Internasional, Refika Aditama; Bandung; 2000 hal. 35.

Hijacking, Threat and use of force Againsts Internationally Protected Person, Taking Of Civilian Hostage, Drug Offenses, International Traffic In Obscene Publication Destruction and/or Theft Of National Treasure, Environmental Protection, Theft Of Nuclear Materials, Unlawful Use Of Mails, Interference of The Submarine Cables, Falcification and Counterfeiting, Bribery of Foreign Public Officials.

Dalam hal pendefinisian kejahatan internasional atau *international crime* sendiri sebagaimana yang telah dikemukakan sebelumnya masih terjadi berbagai macam pertentangan pandangan pakar hukum internasional terhadap kajian cabang hukum internasional ini. Namun dalam pertentangan kajian para pakar tersebut ada beberapa definisi kejahatan internasional yang dapat dikatakan sebagai definisi yang dapat mewakili definisi yang lain.

Menurut Bassiouni definisi dari kejahatan internasional atau *international crime* adalah:

“International crime is any conduct which is designated as a crime in multilateral convention with a significant number of state parties to it, provide the instrument contains one of ten penal characteristics”.

Mungkin masih banyak lagi pendapat para pakar lainnya yang mendefinisikan *international crime*. Akan tetapi menurut pendapat penulis *international crime* itu sendiri terbentuk dari dua unsur yakni *crime* dan *international issue*. Yang mana kedua unsur tersebut dapat didefinisikan sebagai⁹ :

⁹ *Black Law Dictionary*, eight edition, St,Paul MN, Thomson West Publishing Co.,London, 2004,

Crime is an act the law makes punishable, the breach of legal duty treated as the subject matter of criminal proceeding. Also termed criminal wrong.

Sedangkan unsur kedua adalah *international issue* atau masalah internasional adalah berbagai hal – hal yang berkaitan dengan sistem pengaturan terhadap hubungan antar negara, organisasi internasional bahkan individu yang tentu saja bersifat khusus dalam melakukan penanganan terhadap kejahatan yang membahayakan masyarakat internasional.

Oleh karena itulah, adalah suatu keharusan untuk memiliki kemampuan mengidentifikasi jenis – jenis kejahatan yang memiliki implikasi terhadap masyarakat internasional dengan mengenal karakteristik yang dimiliki kejahatan tersebut hingga dapat dikategorikan sebagai suatu kejahatan internasional.

B. Karakteristik Tindak Pidana Internasional

Pada baris terakhir definisi Bassiouni tersebut terdapat frasa yang mengatakan *ten penal characteristics*, atau sepuluh karakteristik kejahatan , dimana karakteristik kejahatan tersebut adalah¹⁰ :

1. *Explicit recognition of proscribed conduct as constituting an international crime or a crime under international law* (pengakuan secara eksplisit tindakan – tindakan yang dipandang sebagai kejahatan berdasarkan hukum kejahatan internasional).

¹⁰ Bassiouni, *International Criminal Law*, Vol, II, *Procedures*, Transnational Publishers, New York, 1986, hal. 3, dikutip dari Romli Atmasasmita, Pengantar Hukum Pidana

2. *Implicit recognition of the penal nature of the act by establishing a duty to prohibit, prevent, prosecute, punish, or the like* (pengakuan secara implisit sifat – sifat pidana dari tindakan – tindakan tertentu dengan menetapkan suatu kewajiban untuk menghukum, mencegah, menuntut, menjatuhkan hukuman atau pidana).
3. *Criminalization of the proscribed conduct* (pidanaan terhadap tindakan tertentu).
4. *Duty or right to prosecute* (kewajiban atau hak untuk menuntut.).
5. *Duty or right to punish to proscribed conduct* (kewajiban atau hak untuk memidanakan tindakan tertentu).
6. *Duty or right to extradate* (kewajiban atau hak untuk melakukan ekstradisi).
7. *Duty or right to cooperate in prosecution , punishment (including judicial assistance in penal proceeding)* kewajiban atau hak untuk bekerja sama didalam penuntutan, pidanaan termasuk bantuan hukum didalam proses pidanaan).
8. *Establishment of criminal jurisdictional basis* (penetapan suatu dasar yurisdiksi kriminal).
9. *Reference to establishment of an international criminal court* (referensi pembentukan suatu pengadilan pidana internasional).
10. *Elimination of defense of superior orders* (penghapusan alasan – alasan perintah atasan).

Akan tetapi pendapat tentang karakteristik kejahatan yang dikemukakan oleh Bassiouni tersebut bukanlah sebuah pendapat yang sempurna. Hal ini ditunjukkan dengan adanya tanggapan Rolling yang mengemukakan bahwa teori yang dikemukakan oleh Bassiouni mengenai karakter penal dari *International Crimes* yang berkaitan dengan diperlukannya sanksi pidana dari sebuah instrumen pemaksa adalah sebuah pendapat yang keliru. Menurut Rolling, penetapan suatu tindakan *international crimes* tidak perlu harus dipandang dari ada atau tidaknya tindakan penjatuhan pidana dalam keadaan nyata. Pendapat itu didasari atas dua hal, *pertama, situasi* (pada saat itu walaupun mungkin hingga

saat ini), yang belum kondusif untuk melaksanakan tindakan penjatuan pidana (bahkan sudah sejak lama pakar – pakar hukum internasional “menghindari” penggunaan instrumen pidana atas tindakan negara yang digolongkan sebagai *international crime*), dan *kedua* perasaan atau kebanggaan nasionalisme yang sangat kuat di kalangan bangsa - bangsa yang merupakan kendala untuk menerima begitu saja yurisdiksi (pidana) internasional.

Meskipun Rolling menyatakan perbedaan pendapat dengan yang dikemukakan oleh Bassiouni terhadap dari salah satu karakteristik kejahatan atau *penal characteristic*, akan tetapi pada dasarnya kedua ahli kejahatan internasional tersebut memiliki kesepahaman mengenai karakter kejahatan yang menginginkan adanya suatu deklarasi internasional yang menegaskan bahwa suatu tindakan dapat digolongkan sebagai kejahatan internasional yang dapat diancam dengan pidana, yang berangkat pada alasan bahwa pada dasarnya yurisdiksi kriminal suatu negara „dibatasi” oleh hukum internasional.

Berdasarkan teori yang dikemukakan oleh Bassiouni dan Rolling tentang kejahatan internasional, maka dapat disimpulkan bahwa pada dasarnya terdapat beberapa unsur yang membedakan suatu perbuatan atau tindakan agar dapat dikategorikan sebagai kejahatan internasional atau bukan. Kriteria pokok tersebut adalah tindakan tersebut mengandung

unsur - unsur mengenai transnasional dan atau internasional serta harus diukur apakah mengandung unsur *necessity element* yang dijabarkan sebagai berikut¹¹ :

1. Unsur internasional, termasuk kedalam unsur ini adalah:
 - a. *Direct threat to world peace and security* (ancaman secara langsung atas perdamaian dan keamanan dunia).
 - b. *Indirect threat to world peace and security* (ancaman secara tidak langsung atas perdamaian dan keamanan dunia).
 - c. *“Shocking To Conscience of humanity* (menggoyahkan perasaan kemanusiaan).
2. Unsur Transnasional, termasuk kedalam unsur ini adalah:
 - a. *Conduct effecting more one state* (tindakan yang memiliki dampak terhadap lebih dari satu negara).
 - b. *Conduct including or affecting citizens of more than one state* (tindakan yang melibatkan atau memberikan dampak terhadap warga Negara dari lebih dari satu negara).
 - c. *Means and methods transcend national boundaries* (sarana dan prasarana serta metode – metode yang digunakan melampaui batas – batas teritorial suatu negara).
3. Unsur *Necessity* (unsur kebutuhan), termasuk kedalam unsur ini adalah, *cooperation of state necessary to enforce* (kebutuhan akan kerjasama antar negara – negara untuk melakukan penanggulangan).

Ketiga unsur tersebut pada dasarnya menunjukkan bahwa tindakan atau perbuatan yang dikategorikan sebagai sebuah kejahatan internasional harus memenuhi persyaratan – persyaratan sebagai sebuah kejahatan yang dapat mengusik rasa aman, kenyamanan dan ketentraman masyarakat bangsa - bangsa atau masyarakat internasional atau “*delicto jus gentium*” serta memenuhi persyaratan bahwa kejahatan tersebut memerlukan penanganan serius secara internasional.

¹¹ Romli Atmasasmita, *Pengantar Hukum Pidana Internasional*, Refika Aditama;

Sehingga setiap negara berhak dan berkewajiban menangkap, menahan, dan menuntut serta mengadili pelaku kejahatan dimanapun kejahatan tersebut dilakukan.

C. *Cyberspace, Cyber Law dan Cybercrime*

Cyberspace, Cyber Law dan Cybercrime merupakan tiga aspek penting dalam melakukan pendalaman dan pemahaman terhadap subjek *hacker* pelaku kejahatan internasional . Sebagaimana kita ketahui ketiga aspek ini memiliki kaitan erat dengan kejahatan internasional (*hacking*) yang dalam pandangan sempit masyarakat sebagai kejahatan yang berkaitan dengan masalah ekonomi. Pada hakikatnya pandangan tersebut sangatlah sempit, pandangan yang sempit inilah yang pada akhirnya mengakibatkan ketidakefektifan penanganan masyarakat internasional terhadap dampak yang jauh lebih besar dari kejahatan ini.

C.1. Cyber Space

Perkembangan teknologi jaringan komputer global atau internet telah menciptakan dunia baru yang dinamakan *Cyberspace*. *Cyberspace* adalah sebuah dunia komunikasi (*computer communication*) yang menawarkan realitas yang baru yaitu realitas virtual . Perkembangan ini membawa perubahan yang mendasar pada tatanan sosial dan budaya masyarakat internasional. Perkembangan *cyberspace* mengubah pengertian tentang masyarakat, komunikasi, komunitas, interaksi social dan budaya.

Dengan menggunakan internet, pengguna dimanjakan untuk menelusuri *Cyberspace* dengan menembus batas kedaulatan, batas budaya, batas agama, suku, ras, politik, ras, hierarki, birokrasi dan lain sebagainya. Hal ini merupakan *smash the boundaries, tear down the hierarchy, and*

dismantle the beureaucracy (para hacker ingin menghilangkan batas- batas kedaulatan negara dengan memperluas *cyberspace*) , sebagaimana dikemukakan oleh Jessica Lipnack dan Jeffry Stamps. Internet juga menjadi sarana yang baik bagi masyarakat dalam pekerjaan, di rumah, maupunditempat – tempat pelayanan publik lainnya sebagaimana dikatakan oleh D.Beckers¹²,

“Information and Communication Technology has invaded all domains of our society : at work, at home and public places. Modern culture is profoundly mediated. Current innovation in computers and telecommunication made new kinds of social interaction and cultural transmission possible across previously imposibble distances. There isa little doubt that this rapid advances in modern telecommunication and computers are changing the way we live our lives, but the direction of change is still uncertain.

Pengertian *cyberspace* tidak terbatas pada dunia yang tercipta ketika terjadi hubungan melalui internet. Setidak – tidaknya dengan memperhatikan definisi tentang *Cyberspace* dari Jhon Perry Barlow, menyebabkan definisi *Cyberspace* lebih luas dari sekedar hubungan melalui internet. Barlow mengemukakan bahwa, ketika sedang melakukan hubungan komunikasi dengan menggunakan telepon atau melakukan aktivitas lain seperti membaca buku, akan timbul sebuah ruang yang dinamakan *Cyberspace*, tetapi ruang yang tercipta itu tidak memungkinkan untuk berinteraksi secara *real time*¹³.

¹² Agus Raharjo, *Cybercrime: Pemahaman dan Upaya pencegahan kejahatan berteknologi*, PT. Citra Aditya Bakti, Bandung, 2002, hal. 91.

¹³ Ibid hal. 92.

Bruce Stirling juga memberikan definisi tentang *Cyberspace* yang mungkin dapat memberikan penjelasan terhadap apa yang dimaksud *cyberspace*. Bruce mengemukakan bahwa¹⁴:

Cyberspace is the "place" where a telephone conversation appears to occur. Not in your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. The place between the phones. The indefinite place out there, where two of you, two human beings, actually meet and communicate.

Dengan merujuk pada hal tersebut, maka sebenarnya *Cyberspace* telah ada ketika Alexander Graham Bell menemukan telepon dan ditemukannya mesin cetak oleh Guttenberg. Meski demikian waktu itu orang tidak menyebut ruang tersebut sebagai *Cyberspace*.

Selain itu Jhon Suller berpendapat bahwa *Cyberspace* merupakan ruang psikologis, yang keberadaannya tidak bergantung pada batas – batas konvensional mengenai benda berwujud. Perbedaan dengan benda dalam dunia nyata adalah *cyberspace* merupakan hasil dari teknologi yang tidak berada dalam dunia nyata akan tetapi memiliki eksistensi sebagaimana Jhon Suller mengungkapkan¹⁵

"Cyberspace is a psychological space. The psychological study of cyberspace as abroad as the field of psychology itself. Anyone who has taken an introductory psychology course known how fast that terrain is Cognitive psychology, personality theory, social psychology, development psychology, clinical psychology are all relevant.

¹⁴ Bruce Stirling, *The Hacker Crackdown, Law and disorder on the electronic frontier*, Massmarket Paperback, 1990, hal 11, yang dapat diakses melalui <http://www.lysator.liu.se/etexts/hacker/>;

¹⁵ Jhon Suller, *The Psychological of cyberspace, overview and guided our September 1999* yang diakses melalui <http://www.rider.edu/user/suler/psycyber.html>. dikutip dari Agus Raharjo, *CYBERCRIME: Pemahaman dan upaya pencegahan kejahatan berteknologi*, PT Citra Aditya Bakti, Bandung 2002. Hal 93

Terlepas dari permasalahan mengenai peristilahan dari *cyberspace*, hal yang tidak kalah pentingnya untuk diperhatikan adalah pada masa kini masyarakat global telah memasuki dunia baru yang didalamnya seseorang dapat melakukan apapun seperti yang dapat dilakukan di dunia nyata, dengan tingkat pengalaman yang sama. Tingkat perkembangan *cyberspace* secara fundamental telah mengaburkan definisi lama tentang ruang fisik identitas dan komunitas¹⁶.

Hubungan ekonomi, komunikasi dan koordinasi yang terjadi didalam *cyberspace* sangat berbeda bila dibandingkan dengan kehidupan nyata atau seseorang melakukan interaksi secara langsung dengan orang lain dengan bertatap muka (*face to face*). Dalam *cyberspace* kita dapat melakukan diskusi mengenai beberapa hal misalnya: berinteraksi dengan teman atau berkenalan dengan orang baru, bahkan merencanakan sebuah kejahatan internasional sekalipun dapat dilakukan dalam dunia yang dapat dikatakan sebagai dunia tanpa batas *Cyberspace* adalah media yang luar biasa untuk melakukan berbagai aktivitas.

C.2 Cyberlaw

Sebagai satu kesatuan yang tak terpisahkan, keberadaan Cyberspace sebagai ruang baru dalam masyarakat tidak hanya memberikan dampak positif terhadap masyarakat internasional (dampak positif tersebut dapat

¹⁶ Mark Slouka, Ruang Yang Hilang, *Pandangan humanis tentang budaya Cyberspace yang merisaukan*, (Mizan,Bandung;1999) , hal 13 dan hal 55, dikutip dari Agus Raharjo, CYBERCRIME: *Pemahaman dan upaya pencegahan kejahatan berteknologi* , PT Citra Aditya Bakti, Bandung 2002. Hal 94

berupa *e-commerce*, *e-government*, jejaring social seperti *Friendster*, *Tagged*, *Facebook*, dan lain - lain, akan tetapi juga memiliki efek yang tidak diinginkan dengan terciptanya ruang tersebut (seperti terjadinya *cyber terrorism*, *virusing*, *spamming*, *carding*, *defacing*, *computer fraud*, dan lain - lain).

Dalam penanggulangan penggunaan negatif dari *cyber space* inilah diperlukan sebuah perangkat khusus dalam mencegah dan melindungi masyarakat dari efek yang dapat ditimbulkan. Dalam hal ini *cyberlaw* memiliki peranan sebagai rambu yang diharapkan dapat menangkal efek negatif dari penggunaan *cyberspace*.

Sebelum melakukan pembahasan yang lebih mendalam mengenai konsep *cyberlaw*, maka perlu kiranya membahas sedikit tentang konsep dasar sumber hukum Internasional. Dalam statute Mahkamah Internasional pasal 38 dikatakan dengan tegas bahwa sumber hukum internasional dalam arti formal antara lain, kebiasaan, perjanjian internasional atau traktat, keputusan pengadilan, atau pendapat para sarjana dan keputusan – keputusan atau resolusi – resolusi organisasi internasional¹⁷. Kelima sumber hukum inilah yang selanjutnya dapat disebut sebagai sumber hukum *cyberlaw* itu sendiri.

¹⁷ I Wayan Patrhiana, *Pengantar Hukum Internasional*, CV Mandar Maju, Bandung, 1990, hal 152.

Meskipun begitu dalam kenyataannya *cyberlaw* sebagai sebuah obyek kajian hukum internasional yang masih sangat baru hanya memiliki perjanjian internasional yakni, *European Council Convention on Cybercrime* (*European treaty series No.185*) dan Resolusi *International Telecommunication Union* (ITU) dan Resolusi Kongres PBB VII pada tahun 1990 sebagai sumber hukum. Sumber hukum tersebut dijabarkan sebagai berikut :

a. Perjanjian Internasional atau Traktat

European Council Convention on Cybercrime (*European Treaty Series No. 185*) yang ditetapkan pada tanggal 23 November 2001 di Budapest. Merupakan perjanjian internasional pertama yang dalam pembuatannya bertujuan untuk melakukan penanggulangan terhadap bahaya *cybercrime* dan pengaturan terhadap internet sebagai media informasi dan komunikasi masyarakat internasional. Pada prinsipnya Konvensi Dewan Eropa ini dibuat dengan tiga tujuan dasar yakni¹⁸ :

1. *Harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime.*
2. *Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offence as well as other offences committed by means of a computer system or evidence in relation which is in electronic form.*
3. *Setting up a fast and effective regime of international cooperation.*

¹⁸ <http://en.wikipedia.org/wiki/convention.on.cybercrime.html> diakses pada hari selasa tanggal 11 januari 2011

Sehubungan dengan uraian diatas hal yang menarik untuk disimak sebagaimana salah satu tujuan dari pembuatan konvensi ini adalah langkah yang ditempuh oleh 41 negara yang tergabung dalam Dewan Eropa dalam melakukan kebijakan harmonisasi hukum pidana untuk menanggulangi kejahatan *cyber* yang dimana tertuang dalam konvensi yang bersifat regional tersebut. Langkah – langkah yang ditempuh oleh Dewan Eropa dalam melakukan harmonisasi adalah¹⁹ :

1. Draf *European Council Convention on Cybercrime* dipersiapkan terlebih dahulu oleh tim ahli atau pakar dalam bidang kejahatan *cyber*.
2. Langkah selanjutnya adalah melakukan sosialisasi terhadap konvensi ini sebagai bahan diskusi publik.
3. Setelah draf konvensi tersebut telah diperbaiki berulang kali dan disetujui oleh negara anggota, draf konvensi tersebut dinyatakan sempurna barulah draf tersebut ditindak lanjuti untuk dituangkan dalam kebijakan legislasi masing – masing negara anggota.

Saat ini konvensi dewan Eropa telah diberlakukan sebagai sebuah kebijakan dalam penanggulangan kejahatan *cyber* di Eropa. Akan tetapi hal yang perlu diketahui bahwa konvensi ini tidak hanya diratifikasi oleh Negara – Negara Eropa melainkan beberapa Negara lainnya yang tidak termasuk dalam wilayah uni - Eropa, seperti, Amerika, Jepang, dan Kanada.

¹⁹ Dikutip dari Barda Nawawi Arief, *Tindak Pidana Mayantara*, perkembangan kajian *cyber* di Indonesia, PT. Rajagrafindo Persada, Jakarta, 2006 , hal 12

b. Keputusan - keputusan atau Resolusi - Resolusi organisasi internasional.

1. Resolusi Kongres PBB VIII/1990 mengenai *Computer Related Crimes* .

Dalam upaya penanggulangan kejahatan *Cyber* Persatuan Bangsa - Bangsa dalam kongres PBB VIII/1990 mengenai *Computer Related Crimes* mengajukan beberapa kebijakan antara lain sebagai berikut²⁰:

1. Mengimbau negara anggota untuk mengintensifkan upaya - upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah - langkah diantaranya :
 - a. Melakukan modernisasi hukum pidana materiil dan hukum acara pidana.
 - b. Mengembangkan tindakan - tindakan pencegahan dan pengamanan komputer.
 - c. Membuat langkah - langkah yang membuat masyarakat, aparat pengadilan dan penegak hukum peka (sensitif) terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer.
 - d. Melakukan upaya - upaya pelatihan bagi para hakim, pejabat, dan para penegak hukum mengenai kejahatan ekonomi dan *Cybercrime*.
 - e. Memperluas *Rules of Ethics* dalam penggunaan komputer dan mengajarkan dalam kurikulum informatika.

²⁰ Ibid hal 2 – 3

- f. Mengadopsi kebijakan perlindungan korban *cybercrime* sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah
 - langkah untuk mendorong korban melaporkan adanya *cybercrime*.
- 2. Menghimbau Negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cybercrime*.
- 3. Merekomendasikan kepada komite pengendalian dan pencegahan kejahatan (*committee on crime prevention and control*) PBB untuk
 - a. Menyebarkan pedoman dan standar untuk membantu anggota untuk menghadapi kejahatan komputer di tingkat regional, nasional dan internasional.
 - b. Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara - cara baru menangani masalah *cybercrime* di masa yang akan datang.
 - c. Mempertimbangkan *cybercrime* sewaktu meninjau pengimplementasian perjanjian ekstradisi dalam bantuan kerjasama dibidang penanggulangan kejahatan.

Garis kebijakan yang dikemukakan dalam resolusi PBB diatas terlihat cukup komprehensif, tidak hanya penanggulangan melalui kebijakan penal (baik hukum pidana materiil maupun hukum pidana formil), tetapi juga kebijakan non penal. Hal menarik dari kebijakan non penal yang dikemukakan dalam resolusi PBB itu ialah upaya pengembangan upaya dan

perlindungan komputer dan tindakan – tindakan pencegahan (*computer security and prevention measure*). Hal ini menjelaskan hadirnya pendekatan *techno-prevention*, yaitu upaya pencegahan terhadap kejahatan yang menggunakan media teknologi khususnya dalam jaringan internet. Sangat disadari tampaknya oleh kongres PBB bahwa *cybercrime* yang terkait erat dengan kemajuan teknologi tidak dapat ditanggulangi dengan pendekatan yuridis semata, tetapi diperlukan suatu konvergensi antara hukum dan teknologi.

Upaya penanggulangan *Cybercrime* juga telah dibahas dalam suatu lokakarya yaitu *workshop on cybercrime related to computer networks* yang dilaksanakan oleh UNAFEI selama berlangsungnya konvensi internasional dalam upaya menjaga keamanan internasional pada masa kini dan di masa yang akan datang.

Dari dua dokumen kongres PBB yang telah dikemukakan, jelas terlihat dominasi keinginan agar negara anggota menggunakan sarana penal. Akan tetapi meskipun kongres PBB telah menghimbau negara tidaklah mudah. Dokumen kongres PBB sendiri mengakui bahwa adanya beberapa kesulitan untuk menanggulangi *cybercrime* dengan menggunakan sarana penal, kesulitan tersebut antara lain sebagai berikut²¹:

²¹ Ibid hal 9

- a. Perbuatan kejahatan yang dilakukan berada dilingkungan elektronik.
Oleh karena itu penanggulangan *cybercrime* memerlukan keahlian khusus, prosedur investigasi, dan kekuatan atau dasar hukum yang mungkin tidak tersedia pada aparat penegak hukum di Negara yang bersangkutan.
- b. *Cybercrime* melampaui batas – batas Negara sedangkan upaya penyidikan atau penegakan hukum selama ini dibatasi dalam wilayah teritorial negara itu sendiri.
- c. Struktur terbuka dari jaringan komputer internasional member peluang kepada pengguna untuk memiliki lingkungan hukum (negara) yang belum mengkriminalisasikan *cybercrime*. Terjadinya data *heavens* (negara tempat berlindung atau singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha negara lain untuk memberantas kejahatan itu.

Dengan memperhatikan kesulitan diatas, maka bukan jaminandengan digunakannya sarana penal oleh suatu negara (yaitu melakukan kriminalisasi dengan membuat perundang – undangan pidana), berarti *cybercrime* dapat ditanggulangi. Namun hal ini tidak mengindikasikan suatu negara tidak perlu mengambil langkah kebijakan legislasi. Patut kiranya diperhatikan pernyataan dalam dokumen kongres PBB X/2000 sebagai berikut²² :

²² Dikutip dari Barda Nawawi Arief, *Tindak Pidana Mayantara*, perkembangan kajian cyber di Indonesia, PT. Rajagrafindo Persada, Jakarta, 2006 , hal 11

Dalam jaringan komputer global, kebijakan kriminal suatu negara mempunyai pengaruh langsung pada masyarakat internasional. Para penjahat *cyber* dapat mengarahkan aktivitas elektroniknya melalui suatu negara yang belum melakukan kriminalisasi terhadap perbuatan itu, maka dari itu dia terlindungi oleh hukum yang berlaku di negara tersebut. Sekalipun suatu negara tidak memiliki kepentingan nasional khusus dalam melakukan kriminalisasi terhadap perbuatan tertentu, seyogyanya dapat dipertimbangkan untuk berbuat demikian agar Negara tersebut tidak menjadi *data heaven* (tempat berlindungnya data) dan menjadi terisolasi secara internasional. Harmonisasi hukum pidana substantif mengenai *cybercrime* merupakan hal yang esensial pada kerjasama internasional harus dicapai diantara berbagai negara yang berbeda.

C.3. Cybercrime

Menurut Dony Arius dalam kamus *hacker* mengemukakan bahwa definisi *cybercrime* adalah upaya untuk memasuki/menyusup dan menggunakan fasilitas komputer tanpa ijin dan melawan hukum dengan atau tanpa menyebabkan perubahan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut²³.

Yang menjadi sebuah pertanyaan adalah apakah langkah yang dapat ditempuh oleh para *security professional* (dapat juga disebut sebagai *ethical hacker*) dalam menjalankan aktivitas *penetration testing* untuk membantu pihak – pihak tertentu dalam melakukan pengujian atau pertolongan lain yang berkaitan dengan keamanan jaringan komputer

²³ Dony Arius, *Kamus Hacker*, Penerbit ANDI, Yogyakarta, hal. 64

dapat dikategorikan sebagai *cybercrime*. Jika kita melakukan analisis terhadap definisi yang dikemukakan oleh Dony Arius maka akan ditemukan unsur penting dalam *cybercrime* itu yang merupakan jalan keluar dari permasalahan yang dihadapi oleh seorang *security professional*.

D. Modus Operandi dan Jenis Serangan Hacker

Secara garis besar modus operandi dan *hacking* yang dilakukan oleh hacker ini dikategorikan dalam tiga metode yaitu :

a. *Physically Hacking*

Physically Hacking adalah metode *hacking* yang menggunakan hardware atau perangkat keras. Metode inilah yang digunakan oleh Jhon Chopper *alias Captain Crunch* yang melakukan *hacking* terhadap telepon dengan tujuan untuk memenangkan hadiah liburan. Metode *hacking* ini memang sangat jarang dilakukan dan kurang familiar di kalangan masyarakat karena jarang terpublikasi secara umum melalui media massa seperti televisi. Metode *hacking* ini dilakukan dengan tujuan untuk melakukan pencarian informasi tertentu dengan cara memasukkan perangkat keras kedalam unit yang digunakan yang ingin dijadikan sebagai korban. *Keylogging* contohnya, seorang keylogger bisa menggunakan *keyboard* milik korbannya untuk mencuri informasi penting yang ia miliki baik itu berupa nomor asuransi, nomor kartu kredit, *password*, dan informasi - informasi penting lainnya. Selain itu kegiatan

phsically hacking ini juga biasa dilakukan oleh *vendor* tertentu yang ingin mengetahui sejumlah informasi yang dimiliki oleh pengguna perangkat yang mereka gunakan seperti lisensi produk, *software* yang digunakan oleh konsumennya. *Phsically hacking* ini juga pernah digunakan oleh salah satu *vendor* pembuat kartu grafis yang menanamkan *Trojan* kedalam kartu grafis yang mereka buat dengan tujuan untuk mengetahui lisensi *software game* yang digunakan oleh konsumen yang mereka miliki.

b. *Logically Hacking*

Metode *logically hacking* adalah metode yang paling sering digunakan oleh para *hacker*. Dikatakan sebagai *logically hacking* sebab alat yang digunakan lebih bersifat abstrak dan sebagian besar efek yang ditimbulkan memiliki sifat yang sama walaupun dapat berimbas kedalam dunia nyata.

Dalam melakukan serangan *logically hacking* seorang *hacker* biasanya dilakukan dalam beberapa tahap. Tahapan penyerangan yang dilakukan oleh seorang *hacker* dalam jaringan komputer dengan menggunakan metode *logically hacking* biasanya terbagi dalam lima tahapan yaitu:²⁴

²⁴S'to, *Certified Ethical Hacker 100% Illegal*, Penerbit Jasakom; Jakarta.2009. hal 7-8

1. *Reconnaissance*

Reconnaissance adalah tahap mengumpulkan data dimana *hacker* akan mengumpulkan semua data sebanyak- banyaknya mengenai target. Data yang dikumpulkan dapat berupa data - data personal atau pribadi atau dapat juga dikatakan sebagai data yang berguna untuk melakukan serangan.

2. *Scanning*

Scanning merupakan titik awal dari dimulainya sebuah serangan *hacker* (*pre-attack*). Melalui proses ini *hacker* akan mencari berbagai kemungkinan yang dapat digunakan untuk mengambil alih komputer korban.

3. *Gaining access*

Hasil dari proses pencarian informasi yang ditemukan dalam kedua proses sebelumnya mulai digunakan dalam tahapan ini. Tahapan inilah yang merupakan suatu peristiwa yang dikategorikan sebagai *cybercrime*. Hal ini dikarenakan dalam tahapan inilah penerobosan (*penetration*) terhadap kelemahan – kelemahan yang dimiliki oleh target. Yang patut diketahui bahwa dalam tahapan ini tidaklah perlu menggunakanteknologi yang „canggih“, seorang *craker* bisa saja menggunakan metode social engineering yang memanfaatkan staf IT yang bermental takut pada atasan.

4. *Maintaining Access*

Setelah mendapatkan akses penuh pada komputer target dalam tahap penerobosan, seorang *hacker* biasanya ingin mendapatkan kekuasaan penuh yang bersifat tetap. Dalam hal ini *maintaining access* sangat diperlukan. Para hacker biasanya melakukan penanaman berbagai aksesoris tambahan seperti *backdoor*, *rootkit*, *Trojan* untuk mempertahankan kekuasaannya terhadap jaringan target.

5. *Covering Tracks*

Untuk melindungi diri *hacker* dari tuntutan pidana maka *hacker* harus menutupi jejak dalam sebuah penerobosan. Biasanya para *hacker* melakukan penghapusan *log file* ataukah membuat *file* atau *directory* dalam komputer korban dalam *mode hidden* (tersembunyi).

Dengan melihat kenyataan pada saat ini dengan semakin pesatnya kemajuan teknologi membuat kita selalu berpikir apakah yang menyebabkan terjadinya kejahatan *cyber* yang dilakukan oleh hacker di dunia yang tujuannya untuk kebutuhan manusia. Banyak pakar yang melakukan pembahasan tentang hacker dan aktivitasnya dalam dunia yang borderless tersebut. Begitu pula dengan faktor yang menyebabkan terjadinya kejahatan *cyber* ini. Secara garis besar faktor yang menyebabkan terjadinya *cybercrime* terdiri atas tiga bagian yaitu:

1. Faktor Intelektual : terkadang timbul dari rasa, keingintahuan, keisengan, mencari kepuasan pribadi dan terkadang hanya ingin

menunjukkan eksistensi seorang *hacker* dalam melakukan rekayasa dan mengimplementasikan kemampuan yang ia miliki. Terkadang pelaku *cybercrime* yang didorong oleh faktor intelektual adalah *newbie* dan *script kiddies* yang merupakan tingkat pemula dan biasanya dijejaki oleh seorang *hacker*.

2. Faktor Ekonomi : dapat dikatakan 60% atau lebih dari setengah kejahatan yang dilakukan *hacker* pada dasarnya merupakan dorongan dari faktor ekonomi. Pelaku kejahatan ini biasanya berasal dari negara – negara berkembang yang memiliki tingkat pendapatan masyarakat yang rendah serta didukung dengan lemahnya system hukum yang berlaku di negara tersebut. Sebagai contoh *cybercrime* yang terjadi akibat faktor dorongan ekonomi adalah *carding* atau pemerasan seperti yang dilakukan oleh seorang anak asal Kanada yang menggunakan inisial *Mafia Boy* dalam aksinya yang melakukan pemerasan terhadap beberapa situs perjudian dan sekaligus mengganggu beberapa situs ternama seperti *Yahoo*.
3. Faktor politik : pelaku kejahatan *cybercrime* yang seperti ini biasa disebut sebagai *Hacktivism*. Kejahatan yang disebabkan oleh faktor politik pada dasarnya merupakan masalah yang paling kritis dibandingkan dengan kejahatan *cybercrime* yang disebabkan oleh faktor ekonomi dan intelektual. Faktor politik dapat menyebabkan seorang *hacker* melakukan serangan bertubi – tubi terhadap situs atau jaringan sebuah negara, contohnya para *hacker* Indonesia

beramai – ramai melakukan aktivitas *hacking* terhadap situs Malaysia yang dianggap mencuri lagu dan kebudayaan salah satu daerah di Indonesia.

E. Definisi dan Aspek – Aspek Pertahanan keamanan

Pemikiran masyarakat awam pada saat ini masih menggunakan istilah atau salah satu aspek dari pertahanan dan keamanan kedalam ranah kemiliteran. Pendapat tersebut tidak berarti sebuah kesalahan, akan tetapi sebuah pandangan yang terlalu sempit terhadap zaman yang serba canggih dan maju seperti saat ini. Oleh karena itu peranan hukum diperlukan untuk meluruskan sebuah paradigma yang sudah mulai menempatkan diri tidak pada tempatnya.

Sifat daluarsa yang dimiliki oleh pendapat tersebut dapat ditunjukkan dalam beberapa keadaan, contohnya pada saat terjadinya serangan *Worm SQL Slammer* yang meluluhlantakkan beberapa infrastruktur yang sangat berpengaruh pada masyarakat. Kerisauan dan rasa tidak aman menjadi akibat dari serangan tersebut. Kerisauan tersebut menjadi indikator setiap negara untuk meningkatkan penjagaan pertahanan dan keamanan yang mereka miliki dari serangan baik itu berasal dari luar maupun dari dalam negara mereka.

Oleh karena itu kita harus merumuskan kembali pemaknaan atas aspek keamanan pertahanan yang tidak hanya merujuk pada kepentingan kemiliteran yang dikaitkan dengan keadaan perang akan tetapi berdasarkan ancaman dan efek yang mempengaruhi negara tersebut. Ancaman itu dapat dikategorikan dalam 3 golongan besar yang didasarkan atas

kepentingan hukum, dimana ketiga golongan tersebut adalah:

- a. Kepentingan hukum perorangan (*Individuale Belangen*).
- b. Kepentingan hukum masyarakat (*Social Belangen*).
- c. Kepentingan hukum Negara (*Staatbelangen*).

Perlindungan terhadap ketiga aspek kepentingan inilah yang sebenarnya sebagai sebuah garis yang bersifat utuh yang merupakansatu kesatuan dari aspek pertahanan dan keamanan suatu negara ini sebenarnya bukanlah sebuah hal yang baru akan tetapi belum dipahami secara lebih mendetail. Sebagai contoh sebenarnya Indonesia telah memasukkan aspek ini kedalam Kitab Undang – Undang Hukum Pidana dalam Bab I sebagai kejahatan terhadap keamanan Negara pada pasal 104 sampai dengan pasal129. Dibentuknya pengelompokan kejahatan tersebut sebenarnya ditujukan untuk melindungi dan menjaga kepentingan hukum atas keselamatan dan keamanan negara dari perbuatan – perbuatan mengancam, mengganggu dan merusak kepentingan hukum negara tersebut.

Objek dari kejahatan terhadap keamanan dan pertahanan ini terdapat dalam berbagai bidang yang salah satunya mencakup aspek pertahanan keamanan yang berhubungan dengan status kemiliteran. Objek – objek tersebut antara lain kepentingan hukum atas keselamatan dan keamanan presiden atau wakil presiden, keamanan pemerintahan dalam melakukan tugasnya, kepentingan yang didasarkan pada keutuhan suatu negara, kepentingan hukum atas rahasia negara, kepentingan hukum atas

pertahanan dan keamanan negara terhadap serangan dari luar maupun dalam baik yang bersifat fisik maupun logika yang kesemuanya itu merupakan sebuah kesatuan yang memiliki sinkronisasi antara satu dengan yang lainnya dan menjadi aspek kritis dalam pertahanan dan keamanan suatu negara.

BAB III

METODE PENELITIAN

A. Lokasi Penelitian

Dalam penulisan proposal penulis mengambil lokasi penelitian di 1 (satu) tempat yaitu:

- Polda Sul-Sel tepatnya di bagian Ditreskrimsus *Cyber Crime*

B. Jenis Data

Jenis data yang diperoleh :

- a. Data primer yakni data dan informasi yang diperoleh melalui internet dan *interview* dengan para pakar hukum dan IT baik secara langsung maupun secara tidak langsung dengan menggunakan telepon, email dan layanan chatting *Yahoo Messenger*.
- b. Data sekunder yaitu data yang diperoleh penulis melalui buku - buku, hasil penelitian, jurnal ilmiah, dan yang diperoleh secara langsung (*hard copy*), maupun yang diperoleh dari hasil pencarian melalui internet (*soft copy*).

C. Teknik Pengumpulan Data

Dalam penelitian ini, penulis menggunakan teknik pengumpulan data berdasarkan, yaitu :

1. Penelitian lapangan (*field research*), dilakukan dengan cara pengamatan langsung di lokasi penelitian untuk memperoleh data yang sebenarnya dengan cara, antara lain :
 - a. Wawancara (*interview*), dilakukan dengan jalan mengadakan wawancara dengan pihak-pihak terkait yaitu nara sumber dan para pakar yang mengerti.
 - b. Observasi (pengamatan), yaitu dengan mengamati secara langsung obyek-obyek yang menjadi sasaran penelitian selama berada di lokasi.
2. Penelitian kepustakaan (*Library Research*), yaitu untuk mengumpulkan data melalui kepustakaan dengan membaca referensi-referensi hukum, peraturan perundang-undangan, karya-karya ilmiah, artikel-artikel dari internet serta dokumen-dokumen yang berhubungan dengan masalah yang dibahas dalam proposal ini untuk memperoleh data sekunder.

D. Analisis Data

Dari data primer dan data sekunder yang telah diperoleh, selanjutnya dianalisis secara kualitatif. Kemudian data tersebut dituliskan secara deskriptif guna memberikan pemahaman yang jelas dan terarah dari hasil penelitian nantinya.

BAB VI

HASIL PENELITIAN DAN PEMBAHASAN

A. Penanggulangan Kejahatan Cyber Dalam Tinjauan Hukum Kejahatan Internasional

Dalam bab sebelumnya penulis mengemukakan bahwa untuk menentukan sebuah kejahatan *cyber* dapat dikategorikan kedalam sebuah kejahatan internasional apabila kejahatan tersebut memenuhi syarat yang dapat diklasifikasikan sebagai sebuah kejahatan yang dikategorikan sebagai *international issue*. *International issue* ini dapat dilihat pada bab sebelumnya dimana Bassiouni mengemukakan sejumlah karakteristik kejahatan internasional yang disebut sebagai “*ten penal characteristics*” dimana *cybercrime* memiliki hampir kesepuluh karakteristik kejahatan internasional.

Selain daripada memenuhi karakteristik yang dikemukakan oleh Bassiouni kejahatan *cyber* pula memiliki unsur – unsur yang menjadi kriteria pokok dari kejahatan internasional baik itu unsur nasional, unsur transnasional dan unsur *necessity*. Penjabaran dari unsur pokok tersebut adalah sebagai berikut:

1. Unsur Internasional

Cybercrime dapat dikatakan sebagai sebuah kejahatan yang memiliki unsur internasional sebab dalam kejahatan ini dapat menghasilkan dampak baik itu secara langsung maupun

secara tidak langsung terhadap orang maupun kelompok atau organisasi seperti halnya sebuah negara.

2. Unsur Transnasional

Selain unsur internasional *cyber crime* juga telah memenuhi unsur transnasional karena kejahatan ini dapat berdampak terhadap stabilitas sebuah negara, kenyamanan dan rasa aman dari warga negara tersebut yang dimana menggunakan metode serta prasarana yang tidak hanya bersumber dari negara pelaku kejahatan *cyber* tersebut akan tetapi bisa juga bersumber dari negara lain.

3. Unsur *Necessity*

Unsur ini adalah unsur yang memiliki peranan penting dalam sebuah penanganan dan penanggulangan terhadap jenis - jenis kejahatan tertentu yang dapat mengakibatkan hilangnya rasa aman. Oleh karena itu dalam kejahatan *cyber* dimana organisasi baik itu yang bersifat regional (*European Council*, *Asean*, dan lain - lain) maupun internasional (PBB, ICPO - INTERPOL) dalam rangka merumuskan sebuah jalan keluar dari masalah yang ditimbulkan dari kejahatan yang disebut sebagai "*borderless crime*".

Terpenuhinya ketiga unsur tersebut telah menggambarkan bahwa diperlukannya kesungguhan dari negara – negara tersebut untuk membangun kerjasama baik itu dari aspek teknis maupun non-

teknis. Kerjasama tersebut diharapkan menjadi sebuah jalan keluar dalam rangka melakukan penanggulangan terhadap kejahatan yang masih bersifat sangat baru dan membutuhkan pendalaman yang lebih lanjut dimasa yang akan datang.

Berikut ini penulis melampirkan data kasus tindak pidana kejahatan Cyber Crime yang di lakukan oleh Hakcer di Wilayah Hukum Kepolisian Daerah Sulawesi Selatan :

Tabel 1
Jumlah Kasus Cyber Crime yang dilakukan Oleh Hacker yang di tangani Oleh Kepolisian Daerah Sulawesi Selatan (Tahun 2019 Sampai Tahun 2021)

No	Tahun	Kasus Yang Masuk	Persentase (%)
1	2019	28	28,57
2	2020	36	50,00
3	2021	22	21,43
Jumlah		86	100,00

Sumber Data: Kepolisian Daerah Sulawesi Selatan, Tahun 2021

Dari data diatas menunjukan bahwa pada tahun 2019 pada Kepolisian Daerah Sulawesi Selatan terdapat 28 kasus yang masuk dengan presentase 28,57%, yang ditangani oleh Subdirektorat *Cybercrime* Ditreskrimsus, tahun 2020 pada Kepolisian Daerah Sulawesi Selatan terdapat 36 kasus yang masuk dengan presentase 50,00% yang ditangani oleh Subdirektorat *Cybercrime* Ditreskrimsus, tahun 2021 pada

Kepolisian Daerah Sulawesi Selatan terdapat 22 kasus yang masuk dengan presentase 21,43% yang ditangani oleh Subdirektorat *Cybercrime* Ditreskrimsus.

Berdasarkan dari data tersebut dapat diamati bahwa penanganan kasus oleh Subdirektorat *Cybercrime* Ditreskrimsus, tetap pada delik pidana terhadap perbuatan para hacker dalam melakukan kejahatan cyber crime dalam penerapan hukumnya serta menyandingkan dengan Undang-Undang Nomor 19 Tahun 2016.

Berkaitan dengan penegakan hukum terhadap tindak pidana Cyber Crime di media sosial kepada pelaku, yang merupakan bagian dari tugas Polri itu sendiri khususnya pada wilayah hukum Kepolisian Daerah Sulawesi Selatan dalam melakukan penegakan hukum terkait dengan tindak pidana Cyber Crime di media sosial. Pada Ditreskrimsus Polda Sulsel terdapat unit khusus untuk menangani tindak pidana khusus, salah satunya yang berkaitan dengan informasi dan transaksi elektronik yang menggunakan media teknologi seperti telepon pintar (*smartphone*), komputer, dan lain sebagainya. Contoh kasus Cyber Crime yang mengarah ke tindak pidana yang pernah ditangani oleh Ditreskrimsus Polda Sulsel, yaitu ada peretasan kartu kredit milik anggota kepolisian Polda Sulsel di Kota Makassar. “Tidak perlu bukti yang banyak , kartu kredit korban sudah cukup menjadi bukti yang kuat bagi kami untuk mempenjarakan si pelaku tersebut” kata Bapak Udiyanto selaku Penyidik di Ditreskrimsus Polda

Sulsel²⁵. Tidak hanya ancaman penjara. Pasalnya, tim Cyber Crime Ditreskrimsus Polda Sulsel baru saja menangkap dua orang warga kota Soppeng yang bertempat tinggal di Makassar tepatnya di sebuah apartement Vida View, Dua warga Soppeng pun diamankan, “RS” (22) dan “AS” (23). Keduanya diamankan tim penyidik Cyber Crime Ditreskrimsus Polda Sulsel usai diketahui melakukan peretasan kartu kredit milik anggota kepolisian Polda Sulsel. Sebagaimana yang diungkapkan oleh Bapak Udiyanto selaku Penyidik di Ditreskrimsus Polda Sulsel, bahwa perbuatan R dan A sudah termasuk dalam pelanggaran ketentuan pidana yakni melanggar pasal 30 UU ITE , ayat (1) dan ayat (2) sebagai berikut : (1) setiap orang dengan sengaja tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun. (2) setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik. (Hasil wawancara dengan Bapak Udiyanto Subdit V Siber Ditreskrimsus Polda Sulsel).

Kepolisian di POLDA Sulawesi Selatan sudah melakukan berbagai upaya-upaya dalam menangani tindak pidana penyebaran berita bohong atau hoax dengan cara usaha yang dilakukan secara preventif dan represif.

²⁵ Hasil Wawancara Kepala Ditreskrimsus Polda Sulsel, 7 September 2021

Upaya-upaya tersebut ialah :

1. Upaya prefentif, merupakan upaya pencegahan sebelum terjadinya tindak pidana kejahatan *cyber crime* yang dilakukan oleh *hacker* dengan cara menghilangkan kesempatan dilakukannya perbuatan tindak pidana tersebut. Hal inidilakukan dengan cara membentuk Satuan Tugas Cyber Patrol (Satgas Cyber Patrol).
2. Upaya represif, adalah upaya yang dilakukan setelah terjadinya tindak pidana kejahatan *cyber crime* yang dilakukan oleh *hacker*, upaya yang dilakukan setelah terjadinya tindak pidana tersebut adalah dengan upaya segera melakukan pemeriksaan proses hukum terhadap pelaku untuk segera dilakukan penjatuhan hukuman sesuai dengan perbuatan pidana yang telah dilakukannya.

Berdasarkan hal tersebut diatas maka penulis dapat simpulkan bahwa dalam upaya pihak Ditreskrimsus Kepolisian Daerah Sulawesi Selatan selaku aparat penegak hukum yang memiliki kewenangan untuk melakukan penegakan hukum terhadap tindak pidana khususnya dalam hal ini tindak pidana *cyber crime*. Pihak Kepolisian Ditreskrimsus Polda Sulsel dalam melakukan penegakan hukum menerapkan upaya preventif serta upaya represif dimana upaya represif ini pihak kepolisan telah

menerapkan sesuai dengan ketentuan perundang-undangan yang berlaku.

B. Efek yang ditimbulkan oleh serangan *Hacker* dan implikasinya terhadap Pertahanan dan Keamanan Negara

Berdasarkan analisis yang dilakukan oleh penulis, tujuan dari kegiatan *hacking* pada dasarnya memiliki tujuan – tujuan tertentu. Secara garis besar tujuan tersebut dapat dikategorikan dalam dua tujuan utama yang pertama melakukan penguasaan atas korban dan melakukan penghancuran sistem atau properti yang dimiliki oleh korban. Kedua tujuan itu dijabarkan sebagai berikut :

1. Penguasaan

Tujuan utama dari kegiatan *hacking* adalah memasuki dan menguasai sistem tersebut untuk dieksploitasi setiap saat. Dalam tahapan *hacking* yang telah dikemukakan sebelumnya, penguasaan masuk dalam tahapan *Maintaining Access* yang merupakan hasil dari *Gaining Access* dimana seorang *hacker* mampu masuk dalam suatu sistem baik itu dengan menggunakan *metode logical* maupun *social engineering*. Dalam penguasaan ini biasanya para *hacker* menanamkan *utility* tertentu seperti backdoor, Trojan horse, maupun *utility* lainnya yang menyebabkan komputer yang dimiliki oleh korbannya dapat setiap saat dieksekusi sesuai dengan perintah *hacker*.

2. Penghancuran

Ketika seorang *hacker* telah sampai pada tahapan *gaining access*, *hacker* sebenarnya memiliki dua pilihan yakni melakukan penguasaan ataukah penghancuran terhadap sistem yang diterobos. Jika seorang *hacker* memiliki tujuan yang panjang terhadap sistem yang ia kuasai maka kemungkinan besar seorang *hacker* akan memilih langkah melakukan penguasaan. Akan tetapi jika tujuannya hanya bersifat sementara biasanya dilakukan pengrusakan terhadap sistem tersebut. Tipe kerusakan yang dapat timbul pada sistem yang diserang oleh *hacker* dapat bersifat sementara atau tetap (*permanent destruction*). Kerusakan yang bersifat permanen biasanya dilakukan dengan metode DOS ataupun DDOS. Kedua serangan tersebut dapat mengakibatkan sebuah sistem komputerisasi menjadi *hang* (penguncian otomatis sebuah sistem jika kapasitasnya melewati batas normal atau merasa terancam) bahkan *crash* (keadaan dimana sebuah sistem komputerisasi mengalami kerusakan berat sehingga peluang untuk pulih sudah tidak ada lagi) yang membutuhkan waktu dan biaya yang tidak sedikit untuk melakukan perbaikan.

BAB V

PENUTUP

KESIMPULAN

Berdasarkan uraian permasalahan di atas dapat disimpulkan bahwa kejahatan cyber crime yang dilakukan oleh hacker rata – rata melakukan kejahatan dengan tehnik phising atau mengirim link kepada korban dengan bertujuan mengambil data milik korban baik melalui e-mail atau pun facebook korban. Media sosial yang sering di akses masyarakat : facebook, whatsapp, Instagram, dan lain-lain. Bentuk informasi yang di dapat melalui media social tersebut adalah data pribadi ataupun informasi umum, biodata, foto, video, informasi kartu kredit (CC), dan lain sebagainya. UU No. 19 Tahun 2016. Pasal 30 ayat (1) UU ITE yang berbunyi *“Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun”*.

SARAN

Tujuan penulisan ini agar dapat menambah wawasan tentang telekomunikasi dan Cyber Crime serta memberi tambahan masukan agar penegakan Hukum Cyber Crime di Indonesia dijalankan secara baik karena sudah sangat meresahkan di berbagai lapisan masyarakat.

DAFTAR PUSTAKA

- Abdul Wahib dan Muhammad Labib, 2005. *Kejahatan Mayantara (Cyber Crime)*, PT Refika Aditama, Jakarta
- Agus Raharjo, 2002. *CYBERCRIME: Pemahaman dan upaya pencegahan kejahatan berteknologi*, PT Citra Aditya Bakti, Bandung.
- Ahmad M. Ramli, *Cyber Law dan Haki dalam Sistem Hukum Indonesia*, (Bandung: PT Refika Aditama, 2006)
- Barda Nawawi Arif, *Pembaharuan*
- Barda Nawawi Arief, 2006. *Tindak Pidana Mayantara*, perkembangan kajian cyber di Indonesia, PT. Rajagrafindo Persada, Jakarta.
- Barda Nawawi Arif, *Batas-batas kemampuan Hukum Pidana Dalam Penanggulangan Kejahatan, Beberapa aspek kebijakan penegakan dan pengembangan hukum pidana*, PT. Citra Aditya Bakti, Bandung, 1998.
- Bruce Stirling, 1990. *The Hacker Crackdown, Law and disorder on the electronic frontier*, Massmarket Paperback, yang dapat diakses melalui <http://www.lysator.liu.se/etexts/hacker>;
- Bryan A. Garner, 2004. *Black Law Dictionary*, eight edition, St, Paul MN,
- Cyber Crime « [X-Database].htm. Diakses pada tanggal 22 November 26, 2021 pukul 13:47
- Dony Arius, *Kamus Hacker*, Penerbit ANDI, Yogyakarta, hal. 64
- Edmon Makarim, SH, S.Kom, LL.M. 2003 *Kompilasi Hukum Telekomunika*
- <http://en.wikipedia.org/wiki/cyberterrorism>, diakses pada tanggal 16 November 2021 di perpustakaan pusat Universitas Hasanuddin dengan menggunakan fasilitas Wi-fi pada pukul 10.30 Wita.
- <http://en.wikipedia.org/wiki/convention.on.cybercrime.html> diakses pada hari selasa tanggal 11 januari 2022

<http://www.maryguin.com/blogtop-5-best-criminal-computer-hackers-all-time> yang diakses pada hari senin 17 januari 2021 pada pukul 17:08

Romli Atmasasmita, 2000. *Pengantar Hukum Pidana Internasional*, Refika Aditama; Bandung.

S"to, *Certified Ethical Hacker 100% Illegal*, Penerbit Jasakom; Jakarta.2009.Thomson West Publishing Co,; London.

Wayan Patrhiana, 1990. *Pengantar Hukum Internasional*, CV Mandar Maju, Bandung.