KEJAHATAN HACKING MELALUI JARINGAN INTERNET DI INDONESIA

OLEH : NOLDY MOHEDE, SH, MH
Dosen Fakultas Hukum Universitas Sam Ratulangi Manado

BAB I
PENDAHULUAN

A. LATAR BELAKANG MASALAH

Internet merupakan suatu teknologi digital yang dengan berbagai kecanggihannya mampu menghubungkan antara satu individu dengan individu yang lainnya melalui jaringan virtual sehingga keduannya dapat berinteraksi secara langsung walaupun tidak secara *face to face*. Dalam bidang teknologi, internet adalah sebuah mahakarya yang sangat luar biasa karena dapat mempertemukan antara individu dengan komponen mesin dalam sebuah jaringan vitual sehingga menghasilkan suatu dunia baru yang disebut sengan dunia maya (*cyberspace*), dimana manusia dapat memerintahkan kepada komponen mesin untuk melakukan sesuatu yang kemudian komponen mesin menginformasikan apa yang telah diinformasikan ke dalam bentuk *audio-visual.*

Seiring dengan perkembangan internet yang begitu pesatnya, disisi lain juga diikuti dengan timbulnya permasalahan baru yang sukar untuk dipecahkan. Selain itu juga internet telah membawa perubahan besar terhadap perilaku dan pola hidup daripada individu yang cenderung untuk memilih melakukan segala sesuatu serba cepat dan serta sapat berinteraksi dengan individu yang lainnya tanpa harus bertatap muka secara langsung. Salah satu hal yang meresahkan para pengguna internet (*netter*) adalah semakin maraknya aktivitas *hacking* yang dilakukan oleh seorang atau sekelompok orang dengan maksud dan tujuan tertentu. Proses Hacking ini sendiri

sangat bervariasi tergantung teknik, keahlian serta perangkat lunak (*software*) dan perangkat keras (*hardware*) yang digunakan .

Melihat hal-hal tersebut hampir seluruh negara di dunia telah merasakan dampak positif dan dampak negatif yang dihasilkan oleh internet. Oleh karena itu, untuk mengantisipasi dampak negatif tersebut serta mengontrol semua aktivitas yang terjadi di dalam jaringan internet maka sebagian besar negara di dunia telah membentuk aturan hukum dengan maksud memberikan tidakan yuridis terhadap pelanggaran maupun kejahatan yang terjadi didalam jaringan internet. Indonesia sebagai negara yang berkembang juga turut merencanankan pembuatan aturan hukum tersebut. Berbagai usaha pemerintah telah diupayakan untuk menghasilkan suatu aturan yang jelas dan tetap, namun pada kenyataannya hingga sampai saat ini belum juga terwujud, hal ini dikarenakan pada dasarnya ruang lingkup dari jaringan internet itu sendiri sangatlah luas serta tidak adanya kesatuan pemkiran dan yang terpenting kurangnya Sumber Daya Manusia (SDM) dimiliki oleh aparat pemerintah.

Hukum bersumber melalui proses interaksi dari berbagai aspek kemasyarakatan (ekonomi, sosial, politik, budaya, dan teknologi) serta mengatur dan membentuk dan menentukan sifat-sifat masyarakat itu sendiri, jadi dapat dikatakan bahwa hukum terbentuk dan membentuk masyarakat. Pada umumnya pengaruh perkembangan teknologi terhadap hukum berhubungan langsung dengan bagaimana cara pemanfaatan dan pendayagunaan dari teknologi itu sendiri, permasalahaanya disini bagaimana kedudukan dan efektivitas dari hukum yang berlaku (hukum positif) terhadap pesatnya perkembangan teknologi yang semakin tidak dapat dikendalikan lagi. Jika dicermati sekilas akan nampak bahwa teknologi berkembang dengan begitu pesatnya dibandingkan dengan hukum yang hanya selalu mengekor.

Memang tidak seorang pun dapat membayangkan sebelumnya bahkan penciptanya sendiri bahwa internet akan menglami perkembangan yang begitu pesatnya sepeti yang telah terwujud sekarang ini. Hingga sekarang ini internet telah menghubungkan hampir seluruh unit komputer yang ada di dunia serta menghasilkan begitu banyak halaman informasi (*web pages*) sehingga memperkaya jaringan

internet itu sendiri. Disamping itu juga internet memberikan berbagai layanan yang diantaranya dalam bisnis (*e-bussines*), perdagangan (*e-trade*), pendidikan (*e-education*), pemerintahan (*e-government*), dan sebagainya yang tentunya layanan-layanan tersebut bersifat praktis dan memudahkan dalam setiap prosesnya.

Seiring dengan perkembangan internet yang begitu pesat, disisi lain juga diikuti dengan timbulnya berbagai permasalahan baru yang sukar untuk dipecahkan dalam bidang teknologi. Selain itu juga internet telah membawa perubahan yang begitu besar terhadap prilaku dan pola hidup individu yang cenderung untuk melakukan segala sesuatu serba cepat serta dapat berinteraksi dengan individu yang lainnya tanpa harus bertatap muka secara langsung. Gejala-gejala tersebut telah membuktikan telah membuktikan bahwa telah adanya dunia lain selain dunia *real* sekarang ini.

Kalaupun ada hukum positif yang telah diberlakukan, akan penggunaan hukum positif tersebut terkadang lebih banyak dilakukan dengan cara penafsiran (*interpretatio*). Melalui pendekatan ini meskipun baik disatu sisi karena semua perubahan yang terjadi di masyarakat dapat diantisipasi. Namun disisi lain, pendekatan seperti ini tidak dapat diterapkan secara terus-menerus karena kedepan nantinya tidak menutup kemungkinan akan menimbulkan kasus yang lain serta menghadirkan penafsiran yang baru pula.

Rencana pembentukan RUU *Cyberlaw* oleh pemerintah Indonesia memang terus diupayakan hingga saat ini, namun masih terbentur dengan perbedaan pendapat dari para penyusun RUU sehingga mengakibatkan timbulnya perdebatan mengenai isi dan bentuknya, karena disatu sisi ada yang berpendapat bahwa cara pengaturannya dapat dilakukan dengan penambahan trhadap aturan hukum positif yang terkait namun ada pula yang berpendapat bahwa untuk melakukan pengaturan dan penindakan mengenai masalah *cyberspace* maka perlu dibauat suatu peraturan yang bersifat *Umbrela Provision*, artinya ketentuan yang dibuat merangkum seluruh permasalahan hukum yang terjadi didalam jaringan internet, kemudian dari *Umbrela Provision* ini dapat dilanjutkan pada ketentuan-ketentuan yang lebih spesifik lagi.

Perkembangan-perkembangan tersebut telah menibulkan pertanyaan mengenai cakupan dari aktivitas hacking yang sering dilakukan oleh para *netter* serta usaha mengantisipasi terhadap pelanggaran-pelanggaran hukum yang dilakukan melalui jaringan internet.

B. PERUMUSAN MASALAH

Bertitik tolak dari uraian yang telah dijelaskan sebelumnya maka dapat ditarik permasalahan sebagai berikut:

1. Apakah yang menjadi cakupan kejahatan hacking melalui jaringan internet di Indonesia ?
2. Bagaimanakah penanggulangan kejahatan hacking melalui jaringan internet di Indonesia ?

C. METODE PENELITIAN

Penelitin ini merupakan penelitian yuridis-normatif, sehingga pengumpulan bahan-bahan yang digumanakan dalam penulisan ini dilakukan melalui Penelitian Kepustakaan (Library Research), yaitu suatu metode yang digunakan dengan jalan mempelajari literatur, perundang-undangan, dan bahan-bahan tertulis lainnya yang berhubungan dengan pembahasan dalam skrpsi ini.

Data yang terkumpul kemudian diolah dengan teknik pengolahan data secara deduksi dan induksi, sebagai berikut:

a. Secara Deduksi, yaitu pembahasan yang bertitik tolak dari hal-hal yang bersifat umum kemudian dibahas menjadi suatu kesimpulan yang bersifat khusus.
b. Secara Induksi, yaitu pembahasan yang bertitik tolak dari hal-hal yang bersifat khusus kemudian dibahas menjadi suatu kesimpulan yang bersifat umum (kebalikan dari teknik deduksi)

D. SISTEMATIKA PENULISAN

Karya ilmiah ini disusun dalam 3 (tiga) bab yang saling berhubungan, karena bab yang diuraikan sebelumnya merupakan dasar untuk uraian dan pembahasan pada bab-bab selanjutnya. Susunan keempat bab tersebut secara garis besar adalah sebagai berikut:

Bab I Pendahuluan, yang menguraikan tentang Latar Belakang Masalah, Perumusan Masalah, Metode Penelitian serta Sistematika Penulisan.

Bab II Merupakan bab pembahasan yang menguraikan mengenai:

A. Cakupan kejahatan hacking melalui jaringan internet di Indonesia
B. Usaha penanggulangan terhadap kejahatan hacking melalui jaringan internet di Indonesia

Bab III Merupakan Bab penutup yang berisikan kesimpulan dan saran dari hasil pembahasan bab sebelumnya

Daftar Pustaka.

BAB II
PEMBAHASAN

A. CAKUPAN KEJAHATAN HACKING MELALUI JARINGAN INTERNET DI INDONESIA

Penggunaan internet di Indonesia baru sebatas hiburan dan percobaan, memang setiap harinya begitu banyak orang yang *log-in* ke internet. Internet pada dasarnya digunakan untuk meningkatkan dan mempercepat proses serta memperlebar jaringan bisnis, sebagai wahana ilmiah untuk mencapai referensi berbagai perpustakaan di seluruh dunia. Namun orang Indonesia secara moral belum siap menghadapi teknologi baru ini.[1]

Teknologi selain membawa keuntungan berupa semakin dipermudahnya hidup manusia, juga membawa kerugian-kerugian berupa semakin dipermudahnya penjahat melakukan kejahatannya. Tekonlogi juga memberi pengaruh yang signifikan dalam pemahaman mengenai kejahatan terutama terhadap aliran-aliran kriminilogi yang menitik beratkan pada faktor manusia, baik secara lahir maupun psikologis.[2]

Meluasnya jaringan global internet mengisyaratkan adanya harapan akan terjadinya perubahan ruang dan jarak. Perkembangan tersebut jga akan menuju pada terbentuknya sistem tingkah laku tertentu melalui unsur-unsur dominan berupa pengalaman dan budaya dalam penggunaan informasi.

---

[1] Utoyo Masudi, ***Kejahatan Komputer Melalui Jaringan Internet Di Indonesia***, makalah pada seminar rutin STIMIK-MDP, Palembang, 1 November 2003, hal.13.

[2] ***Ibid***, hal. 2.

Hacking merupakan permasalahan yang penting dalam jaringan internet global. Memang khususnya di Indonesia aktifitas hacking belum menjadi sorotan masyarakat namun semenjak situs Partai Golkar diserang pada 9 Juli 2006 oleh Iqra Syafaat yang menyebabkan tampilan halaman berubah merupakan peringatan yang keras terutama bagi para aparat pemerintah.

Dalam proses hacking terdapat kode etik yang menjadi patokan bagi para calon *hacker* maupun hacker professional. Kode etik itu adalah sebagai berikut:

a. Akses ke komputer atau apapun yang dapat mengajari anda bagaimana dunia bekerja haruslah tidak terbatas.
b. Semua informasi haruslah gratis (bebas)
c. Jangan pernah percaya kepada otoritas
d. *Hackers* atau siapapun ahruslah dihargai dengan kemampuan hackingnya, bukan dikarenakan bagus criteria sepeti tingaktan, umur dan posisi
e. Kita dapat membuat keindahan dengan komputer
f. Komputer dapat membuat hidup kita lebih baik
g. Seperti lampu 'Aladdin', kita dapat membuat apapun dalam genggaman.[3]

Kode etik tersebut merupakan terjemahan dari seorang hacker pertama yang bernama "*The Mentor*" dan wajib dipegang dalam melakukan aksi hackingnya. Memang seperti telah disampaikan sebelumnya bahwa yang dihargai adalah kemampuan hackinganya bukan tingkatan, umur dan posisi namun orang dengan karya hackingya yang harus didengarkan pendapatnya. Oleh karena itu, semua *hacker* memiliki pandangan yang sama setiap melakukan aksi hackingnya., tetapi walaupun pandangan mereka sama namun motivasinya berbeda-beda. Motivasi-motivasi tersebut adalah sebagai berikut:

a. *Corious*, yaitu ketertarikan untuk menemukan jenis system dan data yang dimiliki oleh targetnya.

[3] http://ezine.echo.or.id/ezinel/all%20aboutz%20%hacking%20h3d87%20a.k.a%20moby.txt. All aboutz hacking,

b. *Malicous*, yaitu berusha untuk merusak sistem yang digunakan *web server* yang di koneksikan

c. *High-Profile Intruder*, yaitu keinginan untuk menggunakan sistem pihak lain sebagai target untuk mempromosikan kemampuannya demi memperoleh popularitas dan ketenaran dimata publik.

d. *Analyzer*, yaitu memonitor jaringan komputer serta mendeteksi kelemahan sebuah ystem computer di jaringan lokal maupun internasional

e. *Password Cracking*, yaitu membuka enkripsi password untuk melewati proteksi sebelum mengambil alih system komputer.

f. *Destruction Device*, yaitu jalan terakhir yang dilakukan dalam proses *hacking* jika semua cara telah dilakukan namun tidak dapat mengambil alih sistem jaringan komputer target maka data-datanya yang akan dihacurkan dengan cara mengirimkan *worm*, *Trojan* maupun *e-mail bomb* dan sebagainya.

Dengan motivasi berbeda-beda tersebut otomatis akibat yang dihasilkan juga bervariasi karena tidak menutup kemungkinan dalam kejahatan *hacking* muncul hal-hal yang baru yang memotivasi seseorang untuk melakukan *hacking* sebab dalam realitas virtual informasi merupakan harta karun berharga dan para penghuni *Cybercpace* (dunia maya) yang memiliki keahlian khusus berusaha untuk mendapatkan serta memanfaatkanya secara illegal.

Khusus mengenai proses hacking memang tidak harus selalu sama karena tergantung pada keahlian yang dimiliki. Namun pada umumnya langkah-langkah yang digunakan sebelum memulai sebuah proses hacking yaitu:

a. *Foot printing* : Proses mencari informasi tentang korban sebanyak-banyaknya. Dilakukan dengan data-data di internet , koran dan lain-lain.

b. *Scanning* : Proses lanjutan dengan menganalisa *service* yang dijalankan di internet. Biasanya dilakukan dengan *ping*, *nmap* dan lain-lain.

c. *Enumeration* : Proses lajutan dengan mencoba koneksi ke mesin target.

d. *Gaining Access* : Percobaan pengambil alihan ke target berdasarkan informasi yang telah didapatkan.

e. *Escalating Privilege* : Meningkatkan hak akses jika telah berhasil masuk ke dalam sistem.

f. *Covering Tracks* : Proses menutupi jejak dengan menghapus segala macam *log* agar tidak terlacak.

g. *Denial of Service* : Setelah segala macam cara gagal dilakukan, biasanya dilakukan serangan terakhir yaitu membanjiri target dengan data sehingga mesian tidak dapat berfungsi. Cara ini biasanya setelah *hacker* putus asa dalam usaha pengambil alihan mesin.

DoS ini sampai saat ini merupakan serangan yang paling susah atau bahkan tidak dapat dicegah.[4]

Selain itu hal terpenting yang perlu diperhatikan yaitu metode-metode hacking untuk mendapatkan hak akses ke dalam sistem komputer yang dimiliki oleh targetnya sehingga menyebabkan kehilangan data-data bahkan sampai kerusakan perangkat lunak (*softwar*e) dan perangkat keras (*harware*) yang trdapat dalam computer. Metode-metode hacking tersebut adalah sebagai berikut:

a. DOS (*Denial of Service*) *attack* : adalah serangan yang dilakukan dengan mengirimkan paket sampah. Hasil dari serangan ini adalah terhentinya layanan server (server down), dikarenakan bandwith penuh. Serangan ini juga mengakibatkan *backbone* dimana server menginduk menjadi macet, bahkan pelayanan menjadi terhenti sama sekali.

b. *Defacing* : jenis serangan ini, adalah dengan mengganti halaman depan suatu situs, atau dengan mengganti isi, baik sebagian atau keseluruhan dengan halaman buatan si penyusup.

[4] S'to, Seni Internet Hacking, Jasakom, Jakarta, 2004, hal. 7.

c. *Spoofing* : Serangan ini dilakukan dengan cara pengalihan alamat IP dari suatu situs ke alamat yang di kehendaki oleh si penyusup. Biasanya dialihkan ke situs porno. Model serangan ini biasanya dilakukan pada situs-situs pemerintah atau institusi lainnya sebagai bentuk protes.
d. *Carding* : Serangan ini biasanya dilakukan oleh para 'pencuri' kartu kredit, dengan tujuan biasa mendapatkan nomor kartu kredit dengan tidak sah.
e. *Database Exploit* : Pencurian database suatu situs e-commerce, sehingga mendapatkan banyak nomor kartu kredit dengan 'Cuma-Cuma'.
f. Pembuatan situs palsu : Modus ini dilakukan dengan menbuat situs *e-commerce* palsu. Sehingga pada saat terjadi transaksi 'fiktif', nomor krtu dan validasi dari pemilik asli bisa di dapatkan dengan mudah.
g. Menggunakan *keylogger* : Cara ini biasa terjadi di warnet atau pada layanan internet umum lainnya. Bisa dilakukan oleh orang dalam atau sesama pengunjung sendiri. Dengan cara menanamkan program *logger* pada PC sasaran. Sehingga, bilamana terjadi transaksi *online*, nomor krtu dan kta sandi (*password*)akan tercatat secara otomatis paa masing-masing PC
h. *Root Compromise* : Metode ini merupakan metode teknis penyusupan tertinggi dibandingkan metode lainnya. Karena menuntut pengetahuan (*skill*), kesabaran dan profesionalisme yang tinggi.[5]

Selain itu juga Dani Firmansyah atau dikenal dengan julukan *Xnuxer*, orang yang telah berhasil menerobos masuk ke dalam sistem komputer Komisi Pemilihan Umum (KPU) memlui jaringan internet menjelaskan teknik-teknik *hacking* yang beberapa diantaranaya pernah digunakan untuk meng-*hack* sistem komputer KPU tersebut. Beberapa teknik tersebut adalah sebagai berikut:

a. Pemanfaatan *local cache*

[5] Internet hacking untuk pemula dengan Masaji-Slax dapat ditermui pada http://opensource.opncrack.or.id/index.php?option=com_content&task=view&id=47&itemid=43&limit=1&limitstart=4

Pada saat kita melihat suatu alamat situs, sebenarnya *browser* kita meminta halaman tersebut kepada web server. *Web server* kemudian mengirimkan kode HTML ke komputer *client. Browser* akan menyimpan halaman ini di komputer *local* sebagai *cache* agar pada saat membutuhkan halaman yang sama tidak perlu memintanaya ke *web server* lagi yang lebih lambat. Setelah itu halaman yang sudah di download ke komputer *client* akan dieksekusi dan ditampilkan ke computer kita.[6]

Halaman *cache* tersebut di*copy* ke *hard disk* kemudian dibuka dengan *notepad*. *Local cache* juga dimanfaatkan oleh *hacker* untuk melihat situs mana saja yang dikunjungi oleh seseorang. Selain itu, *local cache* juga menyimpan banyak sekali informasi karena tanpa disadari *password* juga tersimpan disitu. Untuk mengetahui letak dari *local cache* pada *internet explorer klik menu tools => Internet Options => Settings =>Temporary Internet Files Folder*.

b. Menggunakan SQL (*Structured Query Language*) *Injection*

SQL adalah suatu bahasa yang digunakan untuk mendapatkan atau merubah data didalam relational database. *Statement* SQL yang banyak digunakan pada setiap database sangat beragam dan unik. SQL juga merupakan bahasa *query* yang paling banyak digunakan serta *powerfull*. Biasanya SQL Injection digunakan bersama-sama dengan bahasa pemrograman lainnya seperti Python, ASP, C, C++, Java dan Visual Basic.

c. Menyerang dengan Target XSS (*Cross-Site Scripting*)

XSS atau sering disebut dengan *Cross-Side Scripting* semenjak ditemukan dan dipublukasikan ke *mailing list* Bugtrq (securityfocus.com) pada pertengahan tahun 2002, ratusan situs telah menjadi korban seperti hotmail, yahoo, e-bay serta *software* seperti ISS, apache, dan lain-lain.[7]

---

[6] Ibid, hal. 27.

[7] ***Ibid***, hal 110

Cross-Side Scripting disingkat XSS karena jika disingkat CSS maka akan sama dengan CSS yang sudah sangat dikenal yaitu *Cascading Style Sheets* sebagai pemformat HTML (*HiperText Markup Language*). XSS merupakan kelemahan *software* atau aplikasi yang memenfaatkan input form seperti SQL *Injection*, namun bedanya kalau SQL Injection target penyerangannya adalah *database server* maka target XSS adalah *browser client.*

Teknik-tenik penyerangan tersebut masih dapat melahirkan lebih banyak lagi tenik yang baru lagi berdasarkan kekereatifan dan informasi yang didapatkan dari berbagai sumber, karena seiring dengan perkembangan teknologi dan informasi otomatis juga pelanggaran-pelanggaran yang terjadi dalam *Cyberspace.*

Sedemikian kompleksnya kejahatan yang terjadi melalui jaringan internettentunya membuat kita harus berpikir lrbih keras tentang alternative yang bisa dilakukan untuk menanggulangi berbagai masalah *Cybercrime* khususnya mengenai hacking ini. Meskipun Hukum Pidana sebagai alat terakhir yang digunakan, tetapi pada dasarnya Hukum Pidana bukanlah merupakan alat yang paling ampuh karena penanggulangan kejahatan *hacking* dengan menggunakan Hukum Pidana hanya merupakan pengobatan yang bersifat sementara.

B. USAHA PENANGGULANGAN KEJAHATAN HACKING MELALUI JARINGAN INTERNET DI INDONESIA

Indonesia sampai saat ini masih membahas tentang Rancangan Undang-Undang mengenai *Cybercrime*. Bentuk yang digunakan dalam peraturan tersebut adalah *Umbrela Provision* sehingga ketentuan mengenai *Cybercrime* khususnya yang menyangkut tentang hacking tidak diatur dalam perundang-undangan tersendiri, tetapi secara umum diuraikan dalam Rancangan Undang-Undang Informasi da

Transaksi Elektronik (RUU ITE). Secara umum pasal-pasal yang mengatur tentang ketentuan pidana terdapat dalam pasal 29 – pasal 41.[8]

Selain diatur secara tersendiri dalam pasal 29, sebenarnya pasal-pasal yang lain juga dapat diterapkan terhadap tindakan hacking dalam lingkup *Cybercrime* karena hacking merupakan "*the first crime*" dimana dapat mengubah, menghapus dan menambah data yang ada di dalam sistem komputer melalui jaringan koneksi internet setelah sebelumnya melakukan observasi terhadap seluk-beluk sasarannya.

Tindakan hacking juga diatur secara tegas dalam perturan perundang-undangan lain yaitu pasal 40 Undang-Undang Republik Indonesia nomor 36 tahun 1999 tentang Telekomunikasi yang menegaskan:

" Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasidaalm bentuk apapun".[9]

Sistem perundangan di Indonesia belum mengatur secara khusus mengenai kejahatan hacking. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara hanya dapat diterapkan untuk beberapa kejahatan saja, tetapi ada juga kejahatan yang tidak dapat ditanggulangi oleh undang-undang yang diberlakukan saat ini karena adanya berbagai hambatan dalam upaya penyelidikan terhadap masalah–masalah *Cybercrime* antara lain berkaitan dengan prangkat hukum, kemampuan penyidik, alat bukti dan fasilitas komputer forensik.

Beberapa peraturan yang yang dapat diterapkan antara lain, pasal 22 Undang-Undang Telekomunikasi untuk *illegal access*, pasal 38 Undang-Undang Telekomunikasi untuk sebagian pelanggaran *system interferences* sedangkan pasal 40 Undang-Undang Telekomunikasi untuk penyadapan informasi (*illegal interception*). Bentuk-bentuk kejahatan hacking lainnya dapat diancam dengan ketentuan yang terdapat di dalam KUHP karena perbuatan tersebut sebenarnya merupakan perbuatan yang secara langsung menggunakan komputer sebagai alat dalam pelaksanaanya.

---

[8] Tim Pengajar, Hukum Perdagangan Eleltronik (e-Commerce), Fakultas Hukum Universitas Sam Ratulangi , Manado, 2006, Hal 61.

[9] UURI No.36 Tahun 1999 tentang Telekomunikasi, Perpustakaan elektronik Fakultas Hukum Universitas Sam Ratulangi Manado, http://www.unsrat.ac.id/hukum/uu/uu_36_99.htm

Tidak terbayangkan sebelumnya oleh para pembuat KUHP, pada masa depan akan muncul berbagai tindak pidana dengan modus operasi yang berbeda seperti *hacking*. Hal tersebut dimaklumi karena KUHP kita berdasarkan asas korkodansi, merupakan duplikat dari KUHP Belanda (*Wetboek van Strafrecht*) yang mulai berlaku sejak 1 januari1918, hampir tiga dekade setelah belanda memberlakukannya.

Tentunya KUHP (Kitab Undang-Undang Hukum Pidana) tersebut mengandung unsure-unsur *out of date* dan tidak mampu menangani kejadian yang akan datang. Karena pembuat Undang-Undang Huukm Pidana atau Legislatif hanya melihat tindak pidana yang saat itu atau sebelumnya ada. Legislatif belum berniat untuk mempersiapkan ketentuan yang serba guna.

Sealir dengan perkembangan zaman dewasa ini, kemajuan ilmu pengetahuan dan teknologi semakin mencuat tinggi, sehingga dengan perkebangan dan kemajuan teknologi tersebut, tidak dapat disangkal bahwa berbagai segi kehidupan manusia dipermudah karenanya untuk mencapai berbagai macam tujuan dalam upaya meningkatkan kesejahteraannya.

Namun diamping itu tidak dapat dielakkan timbulnya dampak negatif yang perlu diwaspadai agar kemajuan yang dicapai tidak menjurus kepada timbulnya bencana, ancaman, gangguan, tantangan, apalagi kehacuran terhadap kehudupan manusia itu sendiri. Dengan kata lain, dengan semakin canggihnya kehidupan masyarakat di segala bidang, maka tingkat kriminalitasnya pun semakin tinggi, baik kualitas maupun kuantitas, dengan segala modus operasi yang cukup kompleks pula.[10]

Hubungan antara hukum dan teknologi internet tentu saja akan menjadi hal yang unik. Faktor utama adalah undang-undang itu sendiri harus siap namun dalam kenyataan apabila ada kasus yang baru biasanya kita belum siap menentukan hukumannya. Dunia *Cyber* sebagai manifestasi sistem informasi dan telekomunikasi yang terpadu dalam suatu jaringan global,adalah ruangan tanpa batas yang dapat di isi

[10] Widyopramono, ***Kejahatan Dibidang Komputer***, Pustaka sinar Harapan, JAkart, 1994, Hal.9.

dengan sebanyak mungkin kategori. Baik yang sudah ada, akan ada dan mungkin akan terus berkembang. Hukum dan alat perlengkapanya tentu juga harus berkembang, kesiapan para aparat atau umber daya manusiadari penegak hukum harus ditingkatkan dalam hal ini adalah POLRI.[11]

Untuk mengatasi hal tersebut, jelas diperlukan tindakan Legislatif yang sangat cermat dengan mengingat suatu hal, yakni jangan sampai peraturan perundang-undangan menjadi terpana pada *overlegislate* , yang pada gilirannya justru akan membawa dampak negatif, baik di bidang hukum lainnya maupun di bidang social ekonomi.[12]

Selain itu juga ada beberapa alternatif pemecahan terhadap persoalan-persoalan yang tumbuldalam rangka penanggulangan masalah *Cybercrime* yang dikhususkan pada kejahatan *hacking* melalui jaringan intrnet di Indonesia. Alternatif-alternatif pemecahan tersebut adalah sebagai berikut:

a. Jika ketentuan yang akan dibuat nantinya berupa *Cyberlaw* sebagai umbrela provision, maka yang harus ditempuh adalah membuat peraturan mengenai Cybercrime yang dapat mencakup semua aktivitas yang ada di *Cyberspace* termasuk juga hacking. Karena jenis peraturan ini merupakan perturan yang bersifat khusus, maka semua asas-asas serta berbagai bentuk penafsiran harus diatur juga secara tersendiri. Hal tersebut dikarenakan sifatnya antara *virtual reality* dengan *real life*, engan kata lain dilakukan pemisahan ketentuan pidanan yang mengatur antara aktifitas di *Cyberspace* atau dunia maya dengan kehidupan di dunia nyata seperti sekarang ini.
b. Juka yang akan diperbaharui hanya KUHP dengan cara menambah penafsiran-penafsiran sehingga dapat memperluas serta menjangkau semua

[11] Utoyo Marsudi, ***Kejahatan Komputer Melalui Jaringan Internet***, Makalah pada seminar rutin STIMIK-MDP, Palembang, 1November 2003, hal. 4.

[12] Widyopramono, ***Op-Cit***, hal. 48.

kegiatan yang ada di *Cyberspace*., maka pembuatan peraturan pidana atau peraturan yang mengatur tentang *Cybercrime* sudah tidak diperlukan lagi.

Marjono Reksodiputro mengingatkan juga bahwa seyogyangnya penambahan atau perubahan undang-undang hukum pidana jangan sampai menimbulkan efek sosoial ekonomi serta jangan sampai menimbulkan *over criminalization*. Kepentingan masyarakat sepatutnya mendapatkan perhatian.[13]

Lebih lanjut lagi kriminologi Universitas Indonesia (UI) tersebut mengatakan kita perlu berhemat mempergunakan undang-undang hukum pidana dan apabila memang perlu menciptakan aturan pidana baru agar perumusannya dibatasi jangkauannya. Tentang susunannya ia menyarankan hendaknya memakai kata dan kalimat yang tepat, jangan membuat karet.[14]

Berbicara hukum dalam arti luas, berarti mencakup segala macam ketentuan yang ada baik materi hukum tertulis tertuang dalam peraturan perundang-undangan maupun materi hukum tidak tertulis tertuang dalam kebiasaan maupun praktek bisnis yang berkembang. Sehubungan dengan itu, sistem hukum nasional sesungguhnya tetap berlaku dalam segala aktivitas komunikasi yang dilakukan dalam lingkup *Cyberspace*.[15]

Menyusun suatu regulasi (dalam hal ini dikhususkan pada hukum pidana mengenai hacking) terhadap aktivitas yang sangat kompleks apalagi erat kaitannya dengan teknologi informasi dimana secara teknis Indonesia masih tertinggal merupakan pekerjaan yang tidak mudah. Oleh karena itu, di dalam proses penyusunannya diperlukan kumpulan fakta-fakta serta data statistik yang dapat menjadi dasar untuk penentuan keputusan para pembentuk undang-undang yang berupa suatu peraturan.

---

[13] ***Ibid,*** hal.43.

[14] ***Ibid***

[15] Admin, ***Pengantar Telematika***, Fakultas Hukum Universitas Indonesia Lembaga Kajian Hukum Dan Teknologi, dapat dijumpai pada http://www.law.ac.id/lama/telematika.index.html

Lebih lanjut lagi Sunaryati mengatakan: bagaimanapun setiap bidang hukum yang baru itu akan bersumber pada Pancasila dan Undang-Undang Dasar 1945, berlandaskan undang-undang lain peraturan dalam perundang-undangan, mengembangan Yurisprudensi dan hukum kebiasaan di bidang yang bersangkutan, disamping itu diperlukan keterpaduan dan kesearahan antara pembentuk hukum, pengadilan, aparat penegak hukum, profesi hukum dan masyarakat. Dengan demikian akan menjadi suatu satuan terpadu.[16]

Perkembangan teknologi merupakan suatu faktor yang dapat menimbulkan kejahatan, sedangkan kejahatan itu sendiri telah ada dan muncul sejak permulan zaman sampai sekarang dan masa yang akan datang. Bentuk-bentuk kejahatan yang ada pun semakin bervariasi. Satu hal yang patut diperhatikan bahwa kejahatan sebagai gejala sosial sampai sekarang belum diperhitungkan dan diakui menjadi suatu tradisi atau budaya, padahal jika dibandingkan dengan berbagai budaya yang ada, usia kejahatan tentulah lebih tua. Kejahatan telah diterima sebagai suatu fakta, baik pada masyarakat yang paling sederhana (primitif) maupun masyarakat moderen yang merugikan masyarakat. Kerugian yang dihasilkan itu dapat berupa kerugian dalam arti materil maupun moral. Kerugian materil berupa timbulnya korban kejahatan dan rusak atau musnahnya harta benda serta meningkatnya biaya yang harus dikeluarkan bagi penanggulangannya. Kerugian moral berupa kurang atau hilangnya kepercayaan masyarakat pelaksanaan penegakkan hukum yang dilakukan oleh aparat penegak hukum.[17]

Disamping itu Sahetapy menambahkan bahwa melihat sulitnya pembuktian dan kerugian besar yang mungkin terjadi akibatnya, maka sangat diperlukan produk hukum baru yang dapat menangkal dampak kemajuan teknoligi.[18] Unsur utama yang sangat diperlukan untuk menghasilkan produk hukum baru yaitu dengan melakukan

---

[16] Widyopramono, ***Op-Cit***, hal.44

[17] Utoyo Marsudi , ***Kejahatan Komputer Melalui Jaringan Internet***,Makalah pada seminar rutin STIMIK-MDP, Palembang, 1November 2003, hal. 12-13.

[18] Widyopramono, ***Op-Cit***, hal. 45.

pendekatan lewat teknologi. Pendekatan teknologi merupakan subsistem dari bagian sistem yang lebih besar yaitu budaya, karena teknologi merupakan hasil dari kebudayaan itu sendiri. Pendekatan ini perlu dilakukan untuk membangun atau membangkitkan kepercayaan warga masyarakat terutama para aparat penagak hukumterhadap masalah hacking ini yang kemudian mengajarkan serta menyebarluaskan etika penggunaan media komunikasi melalui pendidikan formal maupun pertemuan-pertemuan seperti seminar.

Ketidakpastian yang dihasilkan oleh hukum beserta para aparat penegaknya dalam menanggulangi kejahatan hacking ini menyebabkan penggunaan teknologi merupakan obat yang ampuh untuk menanggulanginya. Hal tersebut terbukti oleh para korban kejahatan *hacking* yang merasa lebih efektif jika penaggulangan dilakukan dengan menggunakan teknologi, karena saat sistem jaringan komputer diterobos oleh penyusup (*hacker*) maka mereka mengandalkan teknologi untuk memperbaikinya kembali serta memasang pengamanan yang lebih ketat lagi meskipun harganya lebih mahal namun mereka harus melakukan untuk melindungi data-data penting dan menanggulangi serangan berikutnya.

Para *hacker* menemukan surganya di Indonesia karena ketidakpastian pengaturan ini. Keadaan ini diperparah dengan tidak adanya perhatian dari aparat penegak hukum atas tejadinya pelanggaran dan kejahatan yang terjadi di dunia maya ini.

Namun dibalik itu semua, dibidang hukum belum tampak kemajuan dalam hal pengaturan hubungan-hubungan hukum yang terjadi di madia internet ini. Belum satu pun undang-undang yang mengatur secara tegas masalah-masalah yang terjadi di *cyberspace* ini meskipun pelanggaran yang dilakukan semakin banyak dan beragam. Dampak ketidakadaan pengturan ini dirasakan oleh para pengguna internet.[19]

Maka untuk mengisi kekosongan hukum tersebut serta memenuhi kebutuhan masyarakat pengguna internet (*internet global community*) akan keamanan dan

[19] Asril Sitompul, ***Hukum Internet***, PT. Citra Aditya Bakt, Bandung, 2004, hal. xiv.

privasi terhadap sistem maupun data-data yang ada di dalam komputer maka ada beberapa alternatif yang dapat digunakan untuk mangamankan sistem jaringan internet dari para penysup (*hacker*) serta menaggulangi terjadinya kejahatan *hacking* . beberapa alternatif tersebut adalah sebagai berikut:

a. Memasang Proteksi

Dalam menjaga privasi informasi, memasang proteksi merupakan hal utama. Proteksi ini dapat berupa *antivirus* maupun *firewall. Antivirus* digunakan untuk mendeteksi program-program yang dapat merusak sistem-sistem dan data yang ada di dalam komputer, seperti:

1). *Virus*; suatu program atau code yang mengandakan/mereplikasikan dirinya, yaitu menginfeksi program lain, *boot sector*, sektor partisi, atau *document* yang mendukung *macro*, dengan cara memasukkan dirinya atau melampirkan (*attaching*) dirinya ke medium tersebut.
2). *Worm*; suatu progaram yang membuat *copy* dari dirinya sendiri, contohnya darisatu *drive* ke *drive* yang lain, atau meng*copy* dirinya menggunakan e-mail.
3). *Trojan Horse*; suatu program yang tidak mereplikasikan atau mengcopy dirinya, tetapi mengakibatkan kerusakan atau melemahkan keamanan komputer karena pengirim *trojan horse* dapat mengendalikan komputer korban.
4). *Backdoor*; suatu program semacam *trojan horse* dengan kemampuan mencuri data atau *password*.[20]

Lain halnya dengan *firewall*, program ini digunakan untuk memfilter koneksi, *akses*, informasi bahkan *e-mail*. Memang firewall ini melakukan filter secara umum maupun data-data yang diprogramkan terlebih dahulu serta tingkatan kemanan yang diinginkan.

b. Memantau serangan

Seringkali serangan dari penyusup (*hacker*) dilakukan tanpa sepengetahuan dari administrator (*network security*), maka perlu digunakan sistem pemantau terhadap serangan tersebut. Sistem ini dinamakan *Intruder Detection System* (IDS) . secara langsung sistem ini memberikan tanda peringatan kepada administrator berupa

[20] Tim Pengajar, Hukum Perdagangan Eleltronik (e-Commerce), Fakultas Hukum Universitas Sam Ratulangi , Manado, 2006, Hal. 53.

alaram, sinyal bahkan pesan *e-mail* jika adanya serangan. Salah satu contoh IDS yaitu *tcpdump* untuk menganalisis paket apa saja yang lewat [21]

c. Mengatur keamanan program

Saat membuat sistem keamanan jaringan komputer seringkali administrator (*network security*) tidak memperhatikan hal-hal kecil yang dapat dimanfaatkan oleh penyusup (*hacker*), nantinya akan menjadi masalah besar. Oleh karena itu, diperlukan keteliltian dalam membuat suatu program, misalnya pemilihan karakter-karakter khusus yang digunakan untuk pemrograman serta ketelitian perhitungan alogaritma dalam pembuatam program.

d. Menutup service yang tidak diperlukan

Pada umumnya suatu *Operation System* (OS) terdapat layanan (*service*) yang diikutsertakan dan dijalankan secara umum (default). Contohnya seperti Telnet, memlaui *Telnet* ini seseorang dapat berhubungan dengan sedemikian banyak komputer di tempat lain di internet dan secara interaktif dapat mencari berbagai data, *file, software* dan informasi lainnya.[22] Namun dibalik kegunaannya tersebut tanpa disadari layanan ini dapat dimanfaaatkan oleh penyusup (*hacker)* untuk melakukan hacking terhadap suatu *web*, misalnya merubah tampilan halaman situs. Oleh karena itu, jika tidak diperlukan sebaiknya layanan tersebut ditutup.

e. Menggunakan *Publick-Key Cryptogrphy* (Kunci Umum Pengacakan)

Selain sistem, data-data penting yang ada di dalam komputer perlu dijamin keamanannya dengan menggunakan *Publick-Key Cryptogrphy* (Kunci Umum Pengacakan). Dengan bantuan program ini otomstis informasi yang di kirimkan maupun diterima akan diacak (*encrypt*)dan jika ingin membukannya (*decrypt*) diperlukan kata sandi (*password*) yang sebelumnya telah disepakati bersama. kunci umum pengackan ini dilakukan dengan menggunakan *Publick Key Insfrastructures*

---

[21] Chaidir, Belajar Hack Yuck (1)! - ***Konsep Dasar Hacking***, dapat dijumpai pada http://chaidir.wordpress.com/2006/11/08belajar-hack-yuck-bagian-1

[22] Asril Sitompul, ***Hukum Internet***, PT. Citra Aditya Bakt, Bandung, 2004, hal. vii.

yang dimiliki oleh lembaga penyelenggaranyauntuk mendukung Digital Signature (tanda tangan elektronik).

f. Melakukan *Backup*

Mengingat perkembangan kejahatan hacking yang semakin kompleks dan informasi sebagai sasaran utamanya maka dengan melakukan backup secara berkala merupakan suatu alternatif yang sangat diperlukan karena jika penyusup (*hacker*) telah menaklukkan sistem pengamanannya maka selanjutnya yang menjadi sasaran adalah data-data di dalam komputer korban, jika sudah disalin maka ada kemungkinan data-data asli yang ada di dalam komputer korban tersebut akan dirusak atau dimanipulasi sehingga tidak dapat digunakan hal itu dimaksudkan untuk meghilangkan jejak.

Semua usaha yang dilakukan dalam penanggulangan kejahatan hacking melalui jaringan internet di Indonesia baik memamui jalur hukum maupun di luar jalur hukum masing-masing pihak harus memiliki sikap optimis, artinya bagaimanapun dan apapun kejahatan yang telah dilakukan pasti selalu ada jalan keluarnya. Sikap optimis seperti ini harus ditanamkan pada semua pengguna internet baik masyarakat maupun aparat pemerintah. Khusus bagi POLRI sebagai penegak hukum, sikap optimis ini akan mempertajam semangat bahwa semua kejahatan akan diberantas. Di dalam kehidupan ini selalu saja ada kemenangan bagi penegakkan hukum dan keadilan serta tetap ada kekalahan untuk setiap tindak kejahatan.

BAB III
PENUTUP

A. KESIMPULAN

Kesimpulan dalam penulisan karya ilmiah ini adalah sebagai berikut :

1. Hal-hal yang termasuk dalam cakupan kejahatan *hacking* melalui jaringan internet di Indonesia yaitu kode etik, motivasi, langkah-langkah, metode serta teknik *hacking* yang pada umumnya dilakukan oleh para calon *hacker* maupun *hacker* profesional untuk membuat pengrusakan sistem melalui jaringan internet demi mencapai kepuasan, serta menyebarkanb keresahan di kalangan pengguna internet. Hal-hal tersebut juga membuat kejahatan ini menjadi terorganisir dan bahkan hampir tidak dapat ditenggulangi hanya dengan menggunakan peraturan perundang-undangan seperti yang diterapkan sekarang ini.
2. Dalam upaya penagulangan kejahatan *hacking* melalui jaringan internet di Indonesia, pemerintah mengusahakan dua cara melalui jalur hukum yaitu membuat peraturan perudang-undangan yang baru di bidang teknologi informasi berupa *cyberlaw* untuk menambah koleksi ketentuan-ketentuan pidana yang ada memperbaharui ketentuan pidana yang ada untuk memperluas lingkup pengaturan *cyberspace*. Selain itu penaggulangan kejahatan hacking ini dapat terlaksana secara menyeluruh maka dilakukan pendekatan dengan teknologi karena.

B. SARAN

Beberapa saran yang penulis kemukakan dalam kesempatan ini adalah :

1. Para pengguna internet khususnya yang memiliki keahlian di bidang kemanan sistem dapat memanfaatkan kehlian dan teknologi untuk keperluan riset serta menyumbangkan hasil pemikiran demi kemajuan ilmu pengetahuan dan teknologi di Indonesia.
2. Melihat perkembangan jaringan internet yang semakin luas dan sudah digunakan hampir di setiap kegiatan maka penanggulangan kejahatan ini harus dipertegas oleh para aparat penegak hukum supaya teknologi internet dapat dimanfaatkan dengan sebaik-baiknya yang pada akhirnya menghasilkan suatu ”dunia baru” dengan realitas virtual yang penuh dengan harapan-harapan bagi seluruh umat manusia.

DAFTAR PUSTAKA

S'to., ***Seni Internet Hacking***, Jasakom., Jakarta, 2004.

Sitompul, Asril, SH, LLM., ***Hukum Internet***., PT Citra Aditya Bakti, Bandung, 2004

Tim Pengajar**.,** ***Hukum Perdagangan Elektronik (e-commerce)***.,Univrsitas Sam Ratulangi, Manado, 2006.

Utoyo, Marsudi, SH**.,** ***Kejahatan Komputer Melalui Jaringan Internet***, STIMIK, Palembang, 2003.

Widyopramono, SH**.,** ***Kejahatan Dibidang Komputer***, Pustaka Sinar Harapan, Jakarta, 1994.

Soedibroto, Soenarto, SH., **KUHP dan KUHAP**, PT Raja Grafindo Persada, Jakarta, 2003.

Internet:

Admin**, Pengantar Telematika, Fakultas Hukum Universitas Indonesia Lembaga Kajian Hukum Dan Teknologi**, dapat dijumpai pada **http://wwwlaw.ac.id/lama/telematika.index.html**

Admin**, Pengertian Hacking, Cracking, Carding & Hijacking, Chibogacyber Community**, dapat dijumpai pada **http://chiboga.php.us/data1?P=4.html**

Admin**, Sifat Dan Hakekat Alamiah Cyberspace,** dapat dijumpai pada **http://www.elektroindonesia.com/elekto/utama6.html**

_____, All aboutz hacking, dapat dijumpai pada **http://ezine.echo.or.id/ezinel/all%20aboutz%20%hacking%20h3d87%20a.k.a%20moby.txt.**

Aron, **Sejarah Internet Indonesia**, dapat dijumpai pada **http://www.jambur.com/aron/?L=blogs.blog&article=200**

_____, **Awal Internet Indonesia**, dapat dijumpai pada **http://wikihost.org/wikis/indonesiainternet/sejarah_internet_indonesia:awal_internet_indonesia**

Chaidir, **Belajar Hack Yuck !(1) – Konsep Dasar Hacking**, dapat dijumpai pada **http://chaidir.wordpess.com/2006/11/08/belajar-hack-yuck-bagian-1/**

Fickry, **Cyberdemocracy**, juni 2007, dapat dijumpai pada **http://deficry.wordpress.com/2007/06/06/hello-world/**

_____, **Hacking dan cracking**, dapat dijumpai pada **http://students.ukdw.ac.id/~22971797/topik1.htm**

_____, **Internet-Wikipedia, the free encyclopedia**, dapat dijumpai pada **http://en.wikipedia.org/wiki/Internet**

_____, **Kamus Komputer Dan Teknologi Informasi, Internet**, dapat dijumpai pada **http://www.total.or.id/info.php?kk=internet**

_____, **Kamus Komputer Dan Teknologi Informasi, Cyberspace,** dapat dijumpai pada **http://www.total.or.id/info.php?kk=Cyberspace**

Scut (kecoak elektronik), **Hacking – Provit vs (non) provit**, dapat dijumpai pada **http://srang.kecoak.or.id/artikel/provitvsnonprovit.txt**

_____, **Sejarah Internet,** dapat dijumpai pada **http://blog.persimpangan.com/blog/2007/08/04/sejarah-internet**

_____, **Membobol Situs TNP_KPU 2004**, dapat dijumpai pada http:// **wikihost.org/wikis/indonesiainternet/wiki/sejarah_internet_indonesia:24_april_2004_xnuxer_ditangkap**

_____, **Hacker Situs Golkar,** dapat dijumpai pada http:// **wikihost.org/wikis/indonesiainternet/wiki/sejarah_internet_indonesia:hacker_situs_golkar**

_____, **Internet Hacking Untuk Pemula Dengan Masaji-Slax,** dapat dijumpai pada **http://opensource.opencrack.or.id/**

Wikipedia Indonesia,Encyclopedia Bebes Berbahasa Indonesia**, Sejarah Internet**, dapat dijumpai pada **http://id.wikipwdia.org/wiki/Sejarah_Internet/**

Sumber-sumber lain:

Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi

Instruksi Presiden Indonesia Nomor 6 Tahun 2001 Tentang Pemanfaatan Dan Pendayagunaan Telematika Di Indonesia