BAB II

ASPEK HUKUM TENTANG TINDAK PIDANA *CRACKING*, *BOTNET* DAN SISTEM KOMPUTER

A. Tinjauan Hukum Tentang Tindak Pidana *Cracking*

Kebutuhan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui internet pula kegiatan komunitas komersial menjadi bagian terbesar, dan terpesat pertumbuhannya serta menembus berbagai batas negara.

Seiring dengan semakin populernya internet sebagai *the network of the networks*, masyarakat penggunanya (*internet global community*) seakan-akan mendapati suatu dunia baru yang dinamakan *cyber space* sebagaimana dipopulerkan oleh Wiliam Gibson dalam novel *neuromancer* yang merupakan khayalan tentang adanya alam lain pada saat teknologi telekomunikasi dan informatika bertemu[13].

Howard Rheingold menyatakan, *cyber space* adalah sebuah ruang imajiner atau maya yang bersifat artifisial, di mana setiap orang melakukan apa saja yang biasa dilakukan dalam kehidupan sosial sehari-hari dengan cara yang baru[14].

[13] Abdul Wahid dan Mohammad Labib, *Op.Cit*, Hal. 32
[14] *Loc.Cit*

Berkaitan dengan *cyber space* ini, Agus Raharjo mengatakan *cyber space* sesungguhnya merupakan sebuah dunia komunikasi berbasis komputer (*computer mediated communication*). Dunia ini menawarkan realitas baru dalam kehidupan manusia yang disebut dengan realitas *virtual* (maya)[15].

Melalui dunia internet atau disebut juga *cyber space*, apapun dapat dilakukan. Segi positif dari dunia maya ini tentu saja menambah perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Namun dampak negatif pun tidak bisa dihindari. Umumnya suatu masyarakat yang mengalami perubahan akibat kemajuan teknologi, banyak mengalami masalah-masalah sosial. Hal itu terjadi karena kondisi masyarakat itu sendiri yang belum siap menerima perubahan atau dapat pula karena nilai-nilai masyarakat yang telah berubah dalam menilai kondisi lama sebagai kondisi yang tidak lagi dapat diterima[16].

Seiring dengan perkembangan teknologi internet, menyebabkan munculnya kejahatan yang disebut dengan *cyber crime* atau kejahatan melalui jaringan Internet. Munculnya beberapa kasus *cyber crime* di Indonesia, seperti pencurian kartu kredit, cracking beberapa situs, menyadap transmisi data orang lain, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam *programmer* (pemrogram komputer atau pemrogram saja atau pengembang perangkat lunak adalah profesi yang menulis program menggunakan bahasa pemrograman[17]) komputer. Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah

---

[15] *Loc.Cit*
[16] Paul B. Horton dan Chester L. Hunt, *Sosiologi*, Erlangga, Jakarta, 1984, hlm. 237
[17] http://id.wikipedia.org/wiki/Programmer, 12, Mei, 2010, 09.54 WIB

perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya *cyber crime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer.

Istilah *cyber crime* sampai saat ini belum ada kesamaan dalam pendapat, bahkan tidak ada pengakuan baku di dunia internasional. Namun ada yang berpendapat bahwa *cyber crime* sama dengan *computer crime*. Donn Parker mengklasifikasikan kejahatan komputer dari sudut empat peranan komputer. *Pertama, komputer sebagai objek*, dalam hal ini termasuk kasus-kasus perusakan terhadap komputer, data atau program yang terdapat didalamnya atau perusakan sarana-sarana komputer seperti Air Conditioner (AC) dan peralatan listrik yang menunjang operasi komputer. *Kedua, komputer sebagai subjek*. Komputer dapat merupakan atau menimbulkan tempat atau lingkungan untuk melakukan kejahatan, seperti pencurian, penipuan dan pemalsuan yang tidak tradisional akan tetapi yang menyangkut harta-harta benda dalam bentuk baru, yaitu berbentuk pulsa-pulsa elektronis dan guratan-guratan magnetis. *Ketiga, komputer sebagai alat*. Pada beberapa tipe dan cara-cara kejahatan dengan menggunakan komputer, peristiwa kejahatannya kompleks dan sulit diketahui. Salah satu contohnya adalah seseorang yang mengambil warkat-warkat penyetoran dari suatu bank dan mencetak nomor-nomor rekeningnya sendiri dengan tinta magnetis pada warkat-warkat tersebut, yang kemudian diletakan kembali pada tempatnya di bank, dari mana kemudian para nasabah mengambil dan mengisinya sebagai bukti penyetoran. Pada waktu komputer

memproses data pada warkat-warkat tersebut, komputer meng-*crediting* rekening dari oknum itu yang kemudian menarik uangnya dengan cek dari rekeningnya sebelum pada nasabah yang menyetor tadi mengajukan protesnya. *Keempat, komputer sebagai simbol*. Suatu komputer dapat digunakan sebagai simbol untuk melakukan suatu penipuan atau ancaman. Hal ini termasuk suatu penipuan melalui iklan dari suatu biro jodoh yang menyatakan bahwa biro jodoh tersebut memakai komputer untuk membantu korban mencari jodoh, akan tetapi biro jodoh itu sama sekali tidak memakai komputer untuk keperluan tersebut[18].

Banyak perbadaan di antara para ahli dalam mengkasifikasikan kejahatan komputer (*computer crime*). Untuk memudahkan klasifikasi kejahatan komputer tersebut maka dari beberapa klasifikasi dapat disimpulkan[19]:

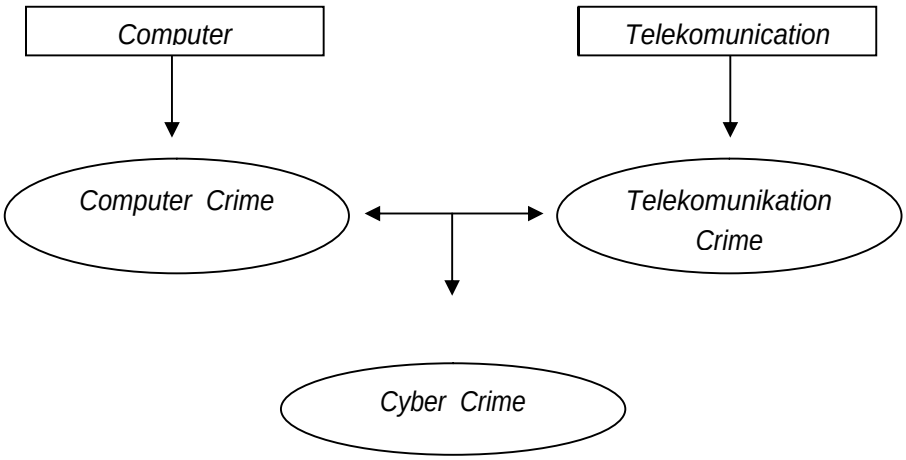
1. Kejahatan-kejahatan yang menyangkut data atau informasi komputer;
2. Kejahatan-kejahatan yang menyangkut program atau software komputer;
3. Pemakaian fasilitas komputer tanpa wewenang untuk kepentingan-kepentingan yang tidak sesuai dengan tujuan pengelolaan atau operasinya;
4. Tindakan-tindakan mengganggu operasi komputer;
5. Tindakan merusak peralatan komputer atau peralatan yang berhubungan dengan komputer atau sarana penunjang.

[18] Abdul Wahid dan Mohammad Labib, *Op.Cit*, Hal. 66-67
[19] *Ibid*, Hal. 67

Dilihat dari keterangan di atas, bahwa *cyber crime* merupakan bagian dari *computer crime*. *Cyber crime* dapat pula disebut sebagai *computer crime*. Untuk lebih jelas dapat dilihat di bagan berikut ini:

Gambar 2.1

Perbedaan *computer crime* dan *cyber crime*[20]



Cyber crime dapat diartikan kejahatan atau tindakan melawan hukum yang dilakukan oleh seseorang dengan menggunakan sarana komputer. Adanya kemajuan internet, di mana komputer-komputer di dunia terhubung satu dengan yang lain, *cyber crime* pun tidak lepas dari peranan internet, atau dengan kata lain, *cyber crime* dapat juga diartikan sebagai kejahatan yang dilakukan di internet atau dunia maya (*cyberspace*).

[20] *Ibid*, Hal. 70

Kejahatan di dunia maya mempunyai karakteristik yang berbeda dengan kejahatan biasa. Beberapa karakteristik dari kejahatan internet adalah sebagai berikut:

1. Kejahatan melintasi batas-batas negara.
2. Sulit menentukan yuridikasi hukum yang berlaku karena melintasi batas-batas negara. Misalnya saja pelaku adalah orang Indonesia yang melakukan transaksi ilegal dari Singapura ke sebuah perusahaan *e-commerce* yang ada di Amerika Serikat dengan menggunakan kartu kredit orang Jepang.
3. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yuridikasi hukum negara mana yang berlaku terhadapnya. Dalam kasus seperti di atas misalnya, hukum negara mana yang harus diberlakukan: Singapura, Amerika Serikat, Jepang atau Indonesia.
4. Menggunakan peralatan-peralatan yang berhubungan dengan komputer dan internet (adanya aliran listrik).
5. Mengakibatkan kerugian yang lebih besar dibanding dengan kejahatan konvensional.
6. Pelaku memahami dengan baik internet, komputer dan aplikasi-aplikasinya.

Menurut Freddy Haris, *cyber crime* merupakan suatu tindak pidana dengan karakteristik sebagai berikut[21]:

1. *Unauthorized access* (dengan maksud untuk memfasilitasi kejahatan);
2. *Unauthorized alteration or destruction of data;*
3. Mengganggu/merusak operasi komputer;
4. Mencegah/menghambat akses pada komputer.

Kejahatan dunia maya atau *cyber crime* pada dasarnya adalah suatu tindak pidana yang mempunyai hubungan dengan ruang dunia maya (*cyber space*), baik yang menyerang fasilitas umum di dalam ruang dunia maya ataupun kepemilikan pribadi. *Encyclopedia of crime and justice*, mendefinisikan *cyber crime* atau kejahatan dunia maya sebagai setiap perbuatan melawan hukum yang memerlukan pengetahuan tentang teknologi komputer yang bertujuan untuk dapat melakukan kejahatan yang dapat dikategorikan dalam dua bentuk, yaitu: penggunaan komputer sebagai alat untuk melakukan suatu kejahatan, seperti pemilikan uang secara ilegal, pencurian properti; atau untuk merencanakan suatu kejahatan, mengunakan komputer sebagai obyek dari suatu kejahatan, seperti sabotase, pencurian atau perubahan data-data milik pihak lain[22].

Adapun jenis-jenis *cyber crime* yaitu:

---

[21] Freddy Haris, Cybercrime Dari Perspektif Akademis, Lembaga Kajian Hukuk dan Teknologi Fakultas Hukum Universitas Indonesia, hlm. 4, dalam (http:www.gipi.or.id), akses tanggal 30 Mei 2004

[22] *Encyclopedia of crime and justice*, New York: Free Press, 1983, (volume 4 hlm. 218-222)

1. *Unauthorized Access to Computer System and Service*

   Kejahatan yang dilakukan dengan menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*cracker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.

2. *Illegal Contents*

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

3. *Data Forgery*

   Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-*

commerce dengan membuat seolaholah terjadi salah ketik yang pada akhirnya akan menguntungkan pelaku.

4. *Cyber Espionage/Data Leakage*

   Kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized* (melalui mekanisme komputer) untuk diambil dan dibocorkan atau melakukan pemerasan.

5. *Cyber Sabotage and Extortion / Data Interference*

   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb* (bom logika adalah bagian dari kode sengaja dimasukan ke dalam perangkat lunak system yang akan memicu fungsi berbahaya ketika kondisi tertentu terpenuhi. Sebagai contoh, seorang programmer dapat menyembunyikan sepotong kode yang dimulai menghapus file seperti sebagai pemicu database gaji, seharusnya mereka pernah dihentikan dari perusahaan[23]), virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan

[23] http://en.wikipedia.org/wiki/Logic_bomb, 11, Mei, 2010, 05.04 WIB

komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau system jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

6. *Offense against Intellectual Property*

   Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

7. *Infringements of Privacy*

   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

8. *Cracking*

Kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang *hacker* dan *cracker* dimana *hacker* sendiri identik dengan perbuatan negatif, padahal *hacker* adalah orang yang memiliki keahlian untuk mempelajari, menganalisa, dan selanjutnya bila menginginkan, bisa membuat, memodifikasi, atau bahkan mengeksploitasi kelemahan sistem perangkat lunak di komputer; biasanya kemudian di publikasikan secara terbuka di Internet agar sistem menjadi lebih baik, sedangkan *cracker* adalah orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang di masuki seperti: merusak data, pencurian data, penghapusan, dan banyak yang lainnya.

9. *Carding*

   Kejahatan dengan menggunakan teknologi computer untuk melakukan transaksi *online* dengan menggunakan nomor kartu kredit orang lain sehingga dapat merugikan orang pemilik asli kartu kredit tersebut baik materil maupun non materil. Nomor-nomor kartu kredit banyak didapatkan dari *program card generator* maupun kegiatan *chat*, *search engine*, dan *milis*. Milis (Inggris: *mailing list*) adalah group diskusi di internet dimana setiap orang bisa berlangganan dan

berikutserta didalamnya. Anggota milis dapat membaca surat dari orang lain dan kemudian mengirimkan balasannya. Secara sederhana, milis adalah sebuah daftar alamat surat elektronik yang mempunyai kesukaan/kepentingan yang sama[24].

Sementara itu, menurut NCIS (Naval Criminal Investigative Service) Inggris, manifestasi dari tindak kejahatan *cyber crime* muncul dalam berbagai macam varian seperti berikut[25]:

1. *Recreational Hacker*. Kejahatan ini dilakukan oleh *netter* tingkat pemula untuk sekedar mencoba kekuranghandalan sistem sekuritas suatu perusahaan.
2. *Cracker* atau *criminal minded hacker*. Pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan financial, sabotase dan pengrusakan data. Tipe kejahatan ini dapat dilakukan dengan bantuan orang dalam, biasanya staf yang sakit hati atau datang dari kompetitor dalam bisnis sejenis.
3. *Political hacker*. Aktifis politis atau lebih populer dengan sebutan hacktivist melakukan perusakan terhadap ratusan *we*b untuk mengkampanyekan programya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendiskreditkan lawannya. Usaha tersebut pernah dilakukan secara aktif dan efisien untuk kampanye

[24] http://id.wikipedia.org/wiki/Milis, 12, Mei, 2010, 09.59 WIB
[25] Abdul Wahid dan Mohammad Labib, *Op.Cit*, Hal. 71-72

anti-Indonesia dalam masalah Timor Timur yang dipelopori oleh Ramos Horta.

4. *Denial of Service Attack*. Serangan *denial of service attack* atau oleh FBI dikenal dengan istilah *unprecedented* tujuannya adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna yang legitimated. Taktik digunakan adalah dengan membanjiri situs *web* dengan data yang tidak penting. Pemilik situs akan banyak menderita kerugian karena untuk mengendalikan atau mengontrol kembali situs *web* memakan waktu lama.
5. *Insider* atau *internal hacker*. Kejahatan ini bias dilakukan oleh orang dalam perusahaan sendiri. Modusnya dengan menggunakan karyawan yang kecewa atau bermasalah dengan perusahaan.
6. *Viruses*. Program penggangagu (*malicious*) dengan penyebaran virus dewasa ini dapat menular melaui aplikasi internet. Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisipkan dirinya sendiri ke sel makhluk hidup. Virus komputer dapat merusak (misalnya dengan merusak data pada dokumen), membuat pengguna komputer merasa terganggu, maupun tidak menimbulkan efek sama sekali[26]. Sebelumnya pola penularan

[26] http://id.wikipedia.org/wiki/virus_komputer, 12, Mei, 2010, 10.07 WIB

virus hanya melalui *floppy disk.* Cakram liuk atau disket (bahasa Inggris: *floppy disk*) adalah sebuah perangkat penyimpanan data yang terdiri dari sebuah medium penyimpanan magnetis bulat yang tipis dan lentur dan dilapisi lapisan plastik berbentuk persegi atau persegi panjang[27]. Virus dalam *file* (merupakan kumpulan dari record2 yang membentuk sebuah data yang akan diproses) dan ter-*download* oleh user bahkan bisa menyebar melalui kiriman *e-mail*.

7. *Piracy*. Pembajakan *software* merupakan *trend* dewasa ini. Pihak produsen *software* dapat kehilangan *profit* karena karyanya dapat dibajak melalui *download* dari internet dan dikopi kedalam *CD-room* yang selanjutnya diperbanyak secara illegal tanpa seizin pemiliknya (penciptanya).
8. *Fraund*. Ini adalah sejenis manipulasi informasi keuangan dengan tujuan mengeruk keuntungan sebesar-besarnya. Sebagai contoh harga saham yang menyesatkan melaui rumor, situs lelang fiktif dan sebagainya.
9. *Gambling*. Perjudian *cyber* yang berskala global. Dari kegiatan ini dapat diputar kembali di negara yang merupakan *tax heaven (surga pajak/bebas pajak)*, seperti *cyman island* merupakan surga bagi *money laundering*, bahkan termasuk Indonesia sering dijadikan sebagai negara tujuan *money laundering*.

[27] http://id.wikipedia.org/wiki/Floppy_disk, 12, Mei, 2010, 10.00 WIB

10. *Pornography and Paedophilia*. Dunia *cyber* selain mendatangkan berbagai kemudahan dengan mengatasi kendala ruang dan waktu juga telah menghadirkan dunia pornografi. Melalui news group, *chat rooms* mengeksploitasi pornografi di bawah umur.
11. *Cyber-stalking*. Adalah segala bentuk bentuk kiriman *e-mail* yang tidak dikehendaki user.
12. *Hate Site*. Situs ini sering digunakan untuk saling menyerang dan melontarkan kata-kata tidak sopan dan vulgar yang dikelola oleh para ekstrimis. Penyerangan terhadap lawan sering menggunakan isu rasial, perang program dan promosi kebijakan atau suatu pandangan.
13. *Criminal Communications*. NCIS telah mendeteksi bahwa internet telah dijadikan sebagai alat yang handal dan modern untuk melakukan komunikasi antar gangster, anggota sindikat obat bius dan komunikasi antar *hooligan* di dunia sepakbola.

Di antara jenis kejahatan yang berkaitan dengan internet tersebut yang paling berbahaya dan dapat menimbulkan dampak yang sangat luas adalah *hacking* (dalam pengertian sebenarnya adalah *cracking*). Kongres PBB X di Wina menetapkan *craking*, sebagai *first crime*. Kejahatan ini memiliki kelebihan-kelebihan di antara yang lainnya secara teknis. Kelebihan kejahatan ini antara lain yaitu, pertama, orang yang dapat melakukan kejahatan jenis ini sudah tentu dapat melakukan kejahatan *cyber crime* yang lain. Kedua, secara teknis dari *cracking* ini kualitas dampak yang dihasilkan lebih serius jika dibandingkan

dengan bentuk-bentuk *cyber crime* yang lain. Untuk menyebarkan gambar porno atau *cyber phornograpy* tidak perlu memiliki kemampuan *cracking*, cukup kemampuan minimal tentang internet[28].

Menurut Agus Raharjo, *cracking* dilakukan dengan melalui tahap-tahap sebagai berikut[29]:

1. Mengumpulkan dan mempelajari informasi yang ada mengenai sistem operasi komputer atau jaringan komputer yang dipakai pada target sasaran. Cara memperoleh informasi ini dapat diperoleh dari orang dalam, atau dengan menggunakan komputer yang tersambung ke internet, untuk memperlancar digunakan program tertentu.
2. Menyusup atau mengakses jaringan komputer target. Hal ini dapat dilakukan dengan menipu atau menaklukan sistem yang ada pada jaringan komputer. Di antara caranya adalah menebak *password*, menyadap *password* dan mengeksploitasi kelemahan sistem sasaran. merupakan kumpulan dari beberapa data yang bersifat pribadi dan diperuntukan hanya bagi yang memiliki hak akses. Data tersebut diinputkan untuk dapat masuk kedalam sebuah proses baik bersifat *integer*, *char* maupun *sting*. Sesuai dengan ketentuan yang telah dibuat sebelumnya dalam proses.
3. Menjelajahi sistem komputer (untuk mengakses lebih tinggi). Dalam aktivitas ini seorang *cracker* akan melihat isi dari sistem dan berkeliling menjelajahi seluruh sistem.

---

[28] Abdul Wahid dan Mohammad Labib, *Op.Cit*, Hal. 83-84
[29] *Ibid*, Hal. 84

4. Membuat *backdoor* dan menghilangkan jejak. Seorang *cracker* akan berusaha agar aksinya tidak diketahui, untuk itu ia melakukan penyamaran atau pengilangan jejak agar tidak terdeteksi. Cara yang paling umum adalah mengedit *file-file log* (catatan aktifitas) pada sistem yang dimasukinya dan menghilangkan semua *entry* (daftar *list*) yang berkaitan dengan dirinya. Selain berfikir untuk menghilangkan jejak *cracker* juga membuat *backdoor* jika suatu saat ia kembali. *Backdoor* atau pintu belakang, dalam keamanan sistem komputer, merujuk kepada mekanisme yang dapat digunakan untuk mengakses sistem, aplikasi, atau jaringan, selain dari mekanisme yang umum digunakan[30]. Pada prinsipnya jalan tembus yang dibuat *cracker* setelah masuk akan digunakan untuk kembali. Contoh pemasangan *backdoor* adalah modifikasi *file host equiv* dan *rhosts* pada sistem UNIX. Unix atau UNIX adalah sebuah sistem operasi komputer yang diawali dari *project Multics* (*Multiplexed Information and Computing Service*) pada tahun 1965 yang dilakukan *American Telephone and Telegraph AT&T*, *General Electric* (GE), dan *Institut Teknologi Massachusetts* (MIT), dengan biaya dari Departemen Pertahanan Amerika (*Departement of Defence Advenced Research Project*, DARPA atau ARPA), UNIX didesain sebagai Sistem operasi yang portable, *multi-tasking* dan *multi-user*[31].

[30] http://id.wikipedia.org/wiki/Backdoor, 12, Mei, 2010, 10.02 WIB
[31] http://id.wikipedia.org/wiki/UNIX, 12, Mei, 2010, 10.03 WIB

Namun dimungkinkan akan ada jenis baru atau modus baru lagi. Ini dikarenakan perkembangan *cyber crime* identik dengan perkembanga teknologi itu sendiri. Sehingga perkembangan teknologi akan terus diikuti oleh perkembangan *cyber crime*.

B. Teori-Teori Mengenai *Botnet* dan Sistem Komputer

Salah satu program baru dan berbahaya yang dapat menyusup dalam jaringan komputer adalah *Botnets.* Program tersebut dapat dikendalikan dari jarak jauh *(remote)* sehingga dapat dioperasikan secara lintas negara (transnasional). Pelaku dan korban dapat berada di negara yang berbeda. Hal inilah yang membuat *botnets* perlu diketahui, dipahami dan diwaspadai oleh pengguna teknologi informasi, khususnya oleh pihak yang bertanggung jawab mengamankan jaringan komputer di lingkungannya.

Ada tiga konsep penting yang perlu dipahami mengenai *Botnets* yaitu[32] :

1. ***Botnets*** adalah istilah untuk kumpulan komputer yang terinfeksi dengan kode-kode kejahatan yang dapat dikendalikan dari jarak jauh melalui infrastruktur perintah dan kendali (*collections of computers infected with malicious code that can be controlled remotely through a command and control infrastructure*);
2. ***Bots*** adalah komputer yang terinfeksi dengan kode kejahatan yang berpartisipasi dalam suatu botnet dan menjalankan perintah dari pengendali botnet (*individual computer infected with malicious code*

[32] Mustrundie.wordpress.com/…/b-o-t-n-e-t-s-ancaman-dan-tantangan-ke-depan/, 4, Mei, 2010, 09.00 WIB

that participates in a botnet and carries out the commands of the botnet controller);

3. ***Bot Herder*** adalah seseorang yang memberi perintah dan mengendalikan beberapa kelompok bots, biasanya untuk suatu keuntungan (*A person that commands and controls groups of bots, often for profit*).

Penggunaan istilah *Bot* berasal dari kata Robot yang berarti *Worker* atau Pekerja. Dalam dunia komputer, *Bot* adalah istilah yang digunakan untuk menjelaskan suatu proses otomatis. *Bots* sering pula secara luas digunakan pada internet untuk tujuan yang beragam. Fungsi *bot* dapat berbeda, dari fungsi mesin pencari sampai *games bots* dan IRC channel *bots* (IRC Bot adalah serangkaian *script* atau sebuah program yang berdiri sendiri yang bertujuan untuk melaksanakan fungsi-fungsi khusus dalam *Internet Relay Chat*[33]). Bahasa *skrip* atau bahasa *skripting* (Bahasa Inggris: *scripting language*) adalah bahasa pemrograman komputer yang diinterpretasikan secara khas dan dapat diketik langsung dari *keyboard* oleh pengguna. *Skrip* berbeda dengan program, karena program harus dikonversi terlebih dahulu secara permanen menjadi berkas biner tereksekusi (yaitu nol dan satu) sebelum dijalankan. *Skrip* tetap dalam bentuk aslinya dan diinterpretasikan perintah per perintah setiap kali dijalankan. *Skrip* diciptakan untuk mempersingkat proses tradisional suntingan-kompilasi-tautan-jalankan (*edit-compile-linking-run*)[34]. Salah satu contohnya yang terkenal adalah

[33] http://id.wikipedia.org/wiki/IRC_Bot, 12, Mei, 2010, 10.04 WIB
[34] http://id.wikipedia.org/wiki/Script, 12, Mei, 2010, 10.03 WIB

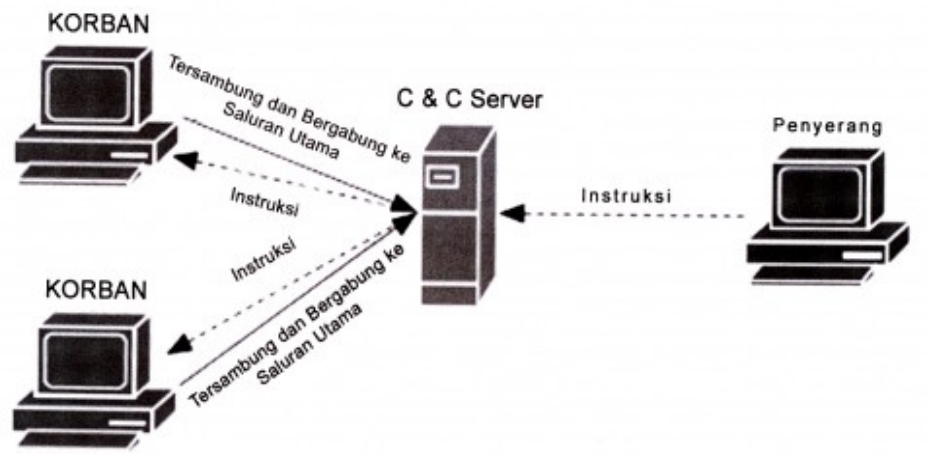
Google bot yang merupakan search *bot*, yang mencari melalui halaman-halaman *web* pada *net* untuk mengumpulkan informasi dan membangun *database* untuk mendapatkan beragam pencarian. Komputer pengontrol lawan atau musuh pada *multiple player video games* juga merupakan salah satu contoh *bot*, di mana proses komputer mencoba meniru tingkah laku manusia[35].

Bots juga dapat digunakan untuk melakukan aktivitas kejahatan *cyber* yang beragam, mulai dari pencurian informasi sampai penggunaan *launching pad*. Pada *launching pad* (pembukaan *pad*) serangan dilakukan secara tersebar, dengan cara meng-*install software* secara tersembunyi tanpa diketahui pengguna komputer yang bersangkutan. Kemudian dari tempat yang terpisah si penyerang *(attacker)* mengendalikan dan memerintahkan mesin yang terinfeksi *bot* untuk melakukan tindakan-tindakan yang dikehendakinya. Alur komunikasi dalam suatu *botnet* dapat digambarkan sebagai berikut :

[35] Mustrundie.wordpress.com/…/b-o-t-n-e-t-s-ancaman-dan-tantangan-ke-depan/, 4, Mei, 2010, 09.00 WIB

Gambar 2.2

Alur komunikasi dalam *botnet*[36]



Seorang *attacker* hanya memerlukan keahlian teknis sederhana untuk dapat menciptakan sebuat *botnet*. Komunitas *attacker* selalu siap membantu dan berbagi pengetahuannya dengan hampir semua orang yang tertarik untuk belajar. Melalui internet, informasi yang tersedia dapat di-*download* setiap saat. Orang yang tidak mengetahui *botnet* dapat memperoleh informasi yang menjelaskan bagaimana menyesuaikan sistem guna memperoleh *packaged exploits* (paket eksploit) dan *command line* (garis perintah) sederhana serta GUI-*run exploit frameworks* (Antarmuka pengguna grafis atau APG Inggris: *Graphical User Interface* atau GUI adalah metoda interaksi secara grafis antara pengguna dan komputer. GUI menjadi salah satu faktor kemudahan dalam penggunaan

[36] Loc.Cit

komputer[37]). Banyak saluran *Internet Relay Chat* (IRC) menawarkan sesi pelatihan dan *advis* kepada *attacker* baru. Cara berbagi pengetahuan seperti ini membantu kesuksesan komunitas *underground*[38].

Botnet, yang diciptakan oleh para *attacker* memerlukan sistem yang rentan untuk eksploitasi. Beberapa daftar jenis IP/*Internet Protocol (netblocks)* yang dipergunakan bersama di antara komunitas *underground* di antaranya[39] :

1. *Netblocks* yang tersedia dengan sistem yang rentan;
2. *Netblocks* yang dijaga secara ketat dan harus dihindari;
3. *Netblocks* yang tidak dialokasi *un-routable;* dan
4. *Netblocks* yang dialokasi untuk beberapa jenis organisasi (contohnya universitas atau pemerintahan).

Pada aksinya *attacker* lebih menyukai koneksi *internet broadband ways-on* dibanding *dial-up,* karena kekuatan koneksi *broadband* lebih besar sehingga memperkuat kapasitasnya untuk membuat *botnet* yang lebih kuat. Beberapa contoh alamat yang populer sebagai target *attacker* di antaranya alamat pendidikan *(.edu)* karena memiliki kapasitas yang sangat kuat dan sering kali lemah pengamanannya. Sedangkan alamat lain yang juga populer adalah alamat militer dan pemerintahan *(.mil* dan *.gov)* dengan berbagai alasan di antaranya pengamanan yang berlapis sehingga kemampuan menembus dinding

[37] http://id.wikipedia.org/wiki/Programmer, 21, Mei, 2010, 10.02 WIB
[38] Mustrundie.wordpress.com/…/b-o-t-n-e-t-s-ancaman-dan-tantangan-ke-depan/, 4, Mei, 2010, 09.00 WIB
[39] Loc.Cit

pengamanan tersebut menjadi suatu prestasi dan kebanggaan sendiri di antara komunitas *underground.*

Salah satu target penyerangan para *attacker* adalah komputer dengan *software* yang lemah. Dengan *software* yang lemah suatu sistem lebih mudah disusupi dan dimanipulasi. *Attacker* berupaya mengkombinasikan beberapa kelemahan untuk memperoleh kendali dari suatu komputer karena hanya dengan kelemahan tunggal, *attacker* tidak dapat memperoleh akses yang diinginkannya. Beberapa kelemahan yang biasa dieksploitasi untuk menyebarkan *bot malware* telah terdokumentasi di antaranya[40] :

1. VU#568148 : Microsoft Windows RPC rentan terhadap *buffer overflow*;
2. VU#753212 : Microsoft LSA Service mengandung *buffer overflow*; DsRolepInitializeLog() function; dan
3. VU# 117394 : Buffer Overflow in Core Microsoft Windows dll.

Perangkat perusak (bahasa Inggris: *malware*, berasal dari lakuran kata *malicious* dan *software*) adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, peladen atau jejaring komputer tanpa izin termaklum (*informed consent*) dari pemilik. Istilah ini adalah istilah umum yang dipakai oleh pakar komputer untuk mengartikan berbagai macam perangkat lunak atau kode perangkat lunak yang mengganggu atau mengusik. Istilah virus komputer terkadang dipakai sebagai frase pemikat (*catch phrase*)

[40] Loc.Cit

untuk mencakup semua jenis perangkat perusak, termasuk virus murni (*true virus*)[41]. Kelemahan-kelemahan tersebut sebenarnya mempunyai kemampuan untuk mencegah eksploitasi, tetapi karena banyak sistem yang tidak diadministrasikan secara baik atau tidak dijaga untuk selalu ter-*uptodate* dengan *paths*-nya, maka mudah diserang dan menghasilkan tingkat kesuksesan yang tinggi bagi para *attacker.*

Cara lain menciptakan *botnet* adalah dengan memanfaatkan *social engineering* yaitu upaya meyakinkan pengguna komputer untuk melakukan aksi yang seharusnya tidak dilakukan. Manusia adalah penghubung yang lemah dalam rantai keamanan sehingga dah dieksploitasi oleh para penjahat *cyber.* Menurut CERT *(Coordination Center Advisory),* saluran komunikasi yang umum digunakan untuk melaksanakan serangan melalui *social engineering* di antaranya aplikasi *email, web browser,* dan *Instant Messaging (IM).* Selain itu, *botnets* juga dapat diperoleh melalui proses *hijacking* yaitu mencuri dari *attacker* lain, *purchasing* atau membeli dari *attacker* lain, atau pun *trading* yaitu para *attacker* saling tukar menukar *botnets* dengan perhiasan, atau benda ekonomis lain bahkan saling menukar *botnets* sesuai kebutuhannya[42].

Melihat cara kerja dan sifat *botnets* yang dapat dikendalikan dari jarak jauh *(remote),* maka terbuka peluang bagi penggunanya untuk dapat melakukan tindakan kejahatan secara *online* tanpa perlu diketahui eksistensinya secara fisik. Penggunaan *botnets* sebagai alat kejahatan pun belum bisa dirasakan akibatnya sebelum tindakan kejahatan terorganisir tersebut selesai dilakukan

[41] http://id.wikipedia.org/wiki/malware, 12, Mei, 2010, 10.05 WIB

[42] Mustrundie.wordpress.com/…/b-o-t-n-e-t-s-ancaman-dan-tantangan-ke-depan/, 4, Mei, 2010, 09.00 WIB

dan mengakibatkan suatu kerugian. Oleh karenanya untuk mengantisipasi penggunaan *botnets* sebagai kejahatan terorganisir online sehingga diperlukan kemampuan, pengetahuan dan pemahaman yang luas tentang *botnets* itu sendiri dan cara kerjanya.

Antisipasi penggunaan *botnets* sebagai kejahatan terorganisir *online* telah menjadi perhatian dari para penegak hukum maupun para pengguna jaringan telekomunikasi dan berbagai pihak yang mempunyai kepentingan dalam bisnis teknologi informasi di berbagai negara. Microsoft Corporation contohnya, suatu perusahaan yang berpusat di Amerika Serikat, telah memperkenalkan visi keamanan berinternet yaitu :

1. Membantu membangun pengalaman *online* yang lebih aman, terjamin dan dapat dipercaya melalui: kerja sama dengan pemerintah dan penegak hukum; pelaksanaan pengamanan yang dapat diandalkan; dan pendidikan luas dan kampanye kesadaran;
2. Kerja sama dengan pemerintah, penegak hukum dan dunia industri untuk melindungi: konsumen dan pengguna internet; usaha *online* resmi; pelayanan dan infrastruktur pemerintah; dan kepentingan masyarakat umum.

Dalam rangka mengantisipasi penggunaan *botnets* sebagai suatu alat kejahatan *cyber*, telah dilaksanakan berbagai konferensi di antaranya yang diadakan di Lyon, Prancis tanggal 24 sampai dengan 28 April 2006 yaitu Konferensi International Botnet Task Force yang keempat, yang juga dihadiri

oleh perwakilan dari Mabes Polri. Pada konferensi tersebut dibahas dan didiskusikan mengenai *botnets* dan pembentukan *Botnet Task Force*. Alasan utama dibentuknya *Botnet Task Force* adalah karena *botnets* merupakan ancaman serius dan berbahaya terhadap pengguna komputer dan jaringan teknologi informasi.

Botnet Task Force yang difasilitasi oleh Microsoft Corporation mempunyai tujuan di antaranya :

1. Mendukung terciptanya suatu badan kerja yang terdiri dari para penegak hukum dari berbagai negara yang berkompeten dan berkualitas untuk menangani masalah-masalah *botnets* dan kode kejahatan;
2. Menciptakan suatu kelompok yang akan berinteraksi satu dengan lainnya dan berpartner dengan Microsoft dengan cara-cara yang efektif untuk melakukan tindakan penegakan hukum kapan pun dan di mana pun jika dimungkinkan;
3. Membangun protocol berbagi informasi tentang kode kejahatan dan *botnets* yang akan melacak tendensi dan target-targetnya.

Untuk tujuan tersebut, berbagai pihak dari berbagai negara turut dilibatkan di antaranya para jaksa, penyidik, spesialis produk ID, pengacara dan ahli hukum, analis kriminal, ahli keamanan/teknologi, ahli forensik, dan sedikitnya 100 karyawan Microsoft ditambah dengan profesional lepas lainnya. Adapun negara-negara yang telah terlibat dalam upaya pembentukan *Botnet Task Force*

di antaranya: Amerika Serikat, Perancis, Hong Kong, Indonesia, India, dan Korea.

Untuk menghindari *botnets* diperlukan peningkatan penerapan *internet safety* (keselamatan berinternet) dalam pengoperasian jaringan komputer melalui internet. *Internet safety* dapat dibagi dalam tiga kelompok yaitu *online security* (keamanan berinternet), *consumer protection* (perlindungan Konsumen) dan *child safety* (Keselamatan anak). Online security meliputi kode jahat, *botnets*, *network hacking*, dan *service disruption*. Perlindungan konsumen meliputi *spam*, *phishing*, *spyware*, pencuri identitas, dan penipuan *online*. Sedangkan keamanan anak meliputi pornografi anak, predator anak dan praktik keamanan untuk anak-anak.

Di Indonesia sendiri kejahatan *online* dengan menggunakan *botnets* sebenarnya telah terjadi diberbagai jenis bisnis yang menggunakan jaringan internet. Sebut saja pencurian data dari komputer yang telah disusupi suatu *botnets*,di mana si *controller* (*attacker*) dapat memberikan perintah secara melawan hukum tanpa disadari oleh si pemilik komputer atau pemilik data/informasi yang sah. Tanpa disadari *attacker* dapat melakukan transaksi sesuai kehendaknya sendiri tanpa hak yang sah. Biasanya hal seperti itu dapat terjadi dalam kasus *carding* (kartu kredit) atau belanja *online*. Tetapi, sampai saat ini secara khusus belum ada kasus *botnets* yang dilaporkan kepada Polri. Walaupun demikian, upaya penegakan hukum dan antisipasi atas setiap jenis kejahatan *cyber* khususnya botnets sebagai suatu kejahatan *online*, tetap menjadi perhatian Polri, di antaranya dengan senantiasa ikut serta dalam upaya

kerja sama dengan berbagai negara maupun dengan berbagai pihak yang berkepentingan dan peduli terhadap ancaman serius penggunaan *botnets* sebagai suatu kejahatan *online* maupun jenis kejahatan *cyber* lainnya.

Perangkat hukum internasional sudah dibentuk dengan adanya beberarapa kongres-kongres PBB, dan hal tersebut wajib untuk diratifikasi oleh negara anggota. Langkah yang ditempuh adalah memasukkan *cyber crime* dalam sistem hukumnya masing-masing.

Pada dua dokumen Konferensi PBB mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal, yaitu *cyber crime* dan *computer related crime*. Dalam *back ground paper* untuk lokakarya Konferensi PBB X/2000 di Wina, Austria istilah *cyber crime* dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit disebut *computer crime*. Kedua, *cyber crime* dalam arti luas disebut *computer related crime*. Secara terperinci dalam dokumen tersebut dinyatakan:

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

Dengan demikian *cyber crime* meliputi kejahatan, yaitu yang dilakukan:

a. dengan menggunakan saranasarana dari sistem atau jaringan komputer (*by means of a computer system or network*) ;
b. di dalam sistem atau jaringan komputer (*in a computer system or network*) ; dan
c. terhadap sistem atau jaringan komputer (*against a computer system or network*).

Berdasarkan definisi tersebut, maka dalam arti sempit *cyber crime* adalah *computer crime* yang ditujukan terhadap sistem atau jaringan komputer, sedangkan dalam arti luas , *cyber crime* mencakup seluruh bentuk baru kejahatan yang ditujukan pada komputer, jaringan komputer dan penggunanya serta bentuk-bentuk kejahatan tradisional yang sekarang dilakukan dengan menggunakan atau dengan bantuan peralatan komputer (*computer related crime)*[43]*.*

Dalam rangka menanggulangi *cyber crime*, Resolusi Kongres PBB VIII/1990 mengenai *Computer Related Crimes* dan *International Industry Congres* (IIIC) 2000 *Millenium Congres* di Quebec pada tanggal 19 September

[43] Laporan Konperensi PBB X/2000, 19-7-2000, hlm.26 : The term **"Computer-related crime"** *had been developed to encompass both the entirely new forms of crime that were directed at computers, networks and their users, and the more traditional form of crime that were now being committed with use or assistance of computer aquipment*., dalam Barda Nawawi Arief, 2001, *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan*, Citra Aditya Bakti, Bandung, hlm. 249 – 250.

2000 dan Kongres PBB mengenai *The Prevention of Crime anda The Treatment of Offenders*, mengajukan beberapa kebijakan antara lain[44]:

1. Menghimbau Negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan computer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
   a. Melakukan modernisasi hukum pidana meteriil dan hukum acara pidana;
   b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
   c. Melakukan langkah-langkah untuk membuat warga masyarakat, aparat pengadilan dan penegak hukum sensitive terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer (*cyber crime*);
   d. Memperluas *rules of ethics* dalam penggunaan computer dan mengajarkannya dalam kurikulum informatika;
   e. Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cybe rcrime*.
2. Menghimbau negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cyber crime*.

[44] Barda Nawawi Arif, *Dalam United Nations (Eighth UN Congress On The Prevention Of Crime And The Treatment Of Offenders Report)*, 1991, hal. 141.??????

3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*committee on Crime Preventon And Control*) PBB untuk :
    a. Menyebarluaskan pedoman dan standar untuk membantu Negara anggota menghadapi *cyber crime* di tingkat nasional, regional dan internasional;
    b. Mengembangkan penelitian dan analisa lebih lanjut guna menemukan cara-cara baru menghadapi problem *cyber crime* di masa depan;
    c. Mempertimbangkan *cyber crime* sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerjasama di bidang penanggulangan kejahatan.

Kebijakan penanggulangan *cyber crime* yang digariskan dalam Resolusi PBB sebagaimana diuraikan di atas cukup komprehensif. Penanggulangan tidak hanya melalui kebijakan penal (hukum pidana meteriil dan formil), tetapi juga kebijakan non penal. Kebijakan non penal yang dikembangkan adalah upaya mengembangkan dan pengamanan perlindungan computer dan tindakan-tindakan pencegahan (*computer security and prevention measures*), yakni tindakan pencegahan dengan teknologi.

Secara internasional, PBB telah menghimbau negara-negara anggota untuk menanggulangi *cyber crime* dengan sarana penal, namun dalam kenyataannya tidaklah mudah. Dokumen Kongres PBB X/2000 sendiri mengakui

bahwa ada beberapa kesulitan dalam menanggulangi *cyber crime* dengan sarana penal, antara lain[45]:

1. Perbuatan jahat yang dilakukan berada di lingkungan elektronik. Oleh karena itu penanggulangan *cyber crime* memerlukan keahlian khusus, prosedur investigasi dan kekuatan/dasar hukum yang mungkin tidak tersedia di Negara yang bersangkutan;
2. *Cyber crime* melampaui batas-batas negara, sedangkan supaya penyidikan dan penegakan hukum selama ini dibatasi dalam wilayah territorial negaranya sendiri;
3. Struktur terbuka dari jaringan komputer internasional memberi peluang kepada pengguna untuk memilih lingkungan hukum (Negara) yang belum mengkriminalisasikan *cyber crime*. Terjadi *data havens* (Negara tempat berlindung/singgahnya data, yaitu negara yang tidak memprioritaskan pencegahan penyalahgunaan jaringan komputer) dapat menghalangi usaha negara lain untuk memberantas kejahatan itu. Persoalan di atas sebenarnya berkaitan dengan kebijakan hukum pidana (*penal policy*). Marc Ancel mendefinisikan kebijakan hukum pidana sebagai ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dalam hal ini hukum pidana) dirumuskan secara lebih baik[46].

---

[45] Barda Nawawi Arif, *Dalam United Nations (Eighth UN Congress On The Prevention Of Crime And The Treatment Of Offenders Report)*, 1991, hal. 9

[46] Wisnusubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer,* Universitas Atmajaya, Yogyakarta, 1999, hal. 3.

Kebijakan hukum pidana terkait erat dengan proses kriminalisasi terhadap suatu perbuatan. Dalam Kongres PBB/X/2000 disebutkan bahwa dalam jaringan komputer global, kebijakan *criminal* negara mempunyai pengaruh langsung pada masyarakat internasional. Para penjahat *cyber* dapat mengarahkan aktifitas elektroniknya melalui suatu negara yang belum melakukan kriminalisasi terhadap kejahatan yang dilakukan itu dan oleh karenaya ia merasa aman dan terlindungi oleh hukum yang berlaku di negara tersebut. Walau pun suatu negara tidak mempunyai kepentingan nasional khusus dalam melakukan kriminalisasi terhadap perbuatan tertentu, sepantasnya dipertimbangkan untuk melakukan langkah sebagai upaya menghindari negara tersebut menjadi *data haven* (tempat berlindungnya data) dan menjadi terisolasi secara internasional. Harmonisasi hukum pidana subtantif mengenai *cyber crime* merupakan hal yang esensial apabila kerjasama internasional harus dicapai oleh beberapa negara yang berbeda[47].

Kekhawatiran terhadap kejahatan mayantara di dunia sebetulnya telah dibahas secara khusus dalam suatu lokakarya (yaitu, "*workshop on crimes to computer networks*") yang diorganisir oleh UNAFEI (United Nations of Asia and Far East Institute for Prevention of Crime and Treatment of Offenders/Lembaga Asia dan Timur Jauh Perserikatan Bangsa-Bangsa untuk Pencegahan Tindak Kriminal dan Perlindungan terhadap Pelanggar) selama kongres PBB X/2000

[47] Barda Nawawi Arief, *Op.Cit.,* hal. 10

berlangsung. Adapun kesimpulan dari lokakarya tersebut adalah sebagai berikut[48]:

1. CRC (*computer related crime*) harus dikriminalisasikan;
2. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat cyber (*cyber crimes*);
3. Harus ada kerjasama antara pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi tempat yang aman;
4. Diperlukan kerjasama internasional untuk menelusuri/mencari para penjahat di internet;
5. PBB harus mengambil langkah/tindak lanjut yang berhubungan dengan bantuan dan kerjasama tekhnis dalam penanggulangannya.

Berdasarkan uraian di atas diketahui bahwa sebenarnya *cybercrime* khususnya kejahatan *cracking* adalah sebuah isu hukum internasional. Perbedaannya adalah di beberapa negara anggota PBB sudah meratifikasi hasil kongres internasional mengenai kejahatan ini dalam sebuah regulasi peraturan perundang-undangan secara khusus, sedangkan di Indonesia belum diatur secara khusus mengenai kejahatan tersebut. Instrumen Hukum Internasional Publik yang mengatur masalah kejatan *cyber* yang saat ini paling mendapat perhatian adalah Konvensi tentang kejahatan *cyber (Convention on Cyber Crime*) 2001 yang digagas oleh Uni Eropa. Konvensi ini meskipun pada awalnya

[48] Teguh Arifiyadi, *Cyber Crime dan Upaya Antisipasinya Secara Yuridis (II),* http://www.depkominfo.go.id/portal/?act=detail&mod=artikel_itjen&view=1&id=BRT06100218 2401, diakses tgl. 05 November 2007.

dibuat oleh organisasi Regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diakses oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan *cyber*.

Negara-negara yang tergabung dalam Uni Eropa *(Council of Europe)* pada tanggal 23 November 2001 di kota Budapest, Hongaria telah membuat dan menyepakati *Convention on Cybercrime* yang kemudian dimasukkan dalam *European Treaty Series* dengan Nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal 5 (lima) negara, termasuk paling tidak ratifikasi yang dilakukan oleh 3 (tiga) negara anggota *Council of Europe.* Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal *(criminal policy)* yang bertujuan untuk melindungi masyarakat dari *cyber crime,* baik melalui undang-undang maupun kerjasama internasional.

Hal ini dilakukan dengan penuh kesadaran sehubungan dengan semakin meningkatnya intensitas digitalisasi, konvergensi, dan globalisasi yang berkelanjutan dari teknologi informasi, yang menurut pengalaman dapat juga digunakan untuk melakukan tindak pidana. Konvensi ini dibentuk dengan pertimbangan-pertimbangan antara lain sebagai berikut :

1. **Pertama,** bahwa masyarakat internasional menyadari perlunya kerjasama antar negara dan Industri dalam memerangi kejahatan *cyber* dan adanya kebutuhan untuk melindungi kepentingan yang sah dalam penggunaan dan pengembangan teknologi informasi.
2. **Kedua***,* Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan

kriminal. Hal lain yang diperlukan adalah adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat.

3. **Ketiga**, saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Azasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik Dan sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi/pendapat.

Konvensi ini telah disepakati oleh Masyarakat Uni Eropa sebagai konvensi yang terbuka untuk diakses oleh negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrumen Hukum Internasional dalam mengatasi kejahatan *cyber*, tanpa mengurangi kesempatan setiap individu untuk tetap dapat mengembangkan kreativitasnya dalam pengembangan teknologi informasi.

Istilah komputer mempunyai arti yang luas dan untuk orang yang berbeda. Istilah komputer (*computer*) diambil dari bahasa latin *computare* yang berarti menghitung (*to compute* atau *reckon*)[49].

[49] Jogianto Hartono, *Pengenalan Komputer*, Penerbit: Andy, Yogyakarta, 2000, hal 1-2

Menurut buku *Computer Annual* (Robert H. Blissmer), komputer adalah suatu alat elektronik yang mampu melakukan beberapa tugas sebagai berikut[50]:

1. Menerima *input*,
2. Memproses *input* tadi dengan programnya,
3. Menyimpan perintah-perintah dan hasil dari pengolahan,
4. Menyediakan *output* dalam bentuk informasi.

Menurut buku *Computer Today* (Donald H. Sanders), komputer adalah sistem elektronik untuk memanipulasi data yang cepat dan tepat serta dirancang dan diorganisasikan supaya secara otomatis menerima dan menyimpan data *input*, memprosesnya dan menghasilkan *output* di bawah pengawasan suatu langkah-langkah instruksi-instruksi program yang tersimpan di *memory* (*stoned program*)[51].

Menurut buku Computer Organization (V.C. Hamacher, Z.G. Vrannesik, S.G. Zaky), komputer adalah mesin penghitung elektronik yang cepat menerima informasi input digital memprosesnya sesuai dengan suatu program yang tersimpan dimemorinya (*stoned program*) dan menghasilkan output informasi[52].

Meurut buku Introduction To Computers (Gordon R. Davis), komputer adalah tipe khusus alat penghitung yang mempunyai sifat tertentu yang pasti[53]. Sedangkan yang disebut program adalah kumpulan dari instruksi atau perintah

[50] *Loc.Cit*
[51] *Loc.Cit*
[52] *Loc.Cit*
[53] *Loc.Cit*

terperinci yang sudah dipersiapkan supaya komputer dapat melakukan fungsinya dengan cara yang sudah tertentu.

Supaya Komputer dapat digunakan untuk mengolah data, maka harus berbentuk sistem komputer (*computer system*). Sistem adalah jaringan dari pada elemen-elemen yang saling berhubungan membentuk suatu kesatuan untuk melaksanakan suatu tujuan pokok dari sistem tersebut[54].

Tujuan pokok dari sistem komputer adalah mengolah data untuk menghasilkan informasi. Supaya tujuan pokok tersebut, maka harus ada elemen-elemen yang mendukungnya. Elemen-elemen dari sistem komputer adalah *software, hardware* dan *brainware*[55].

Hardware (perangkat keras/peranti keras) adalah peralatan di sistem komputer yang secara fisik terlihat dan dapat dijamah. *Software* (perangkat lunak/peranti lunak) adalah program yang berisi perintah-perintah untuk pengolahan data. *Brainware* adalah manusia yang terlihat didalam mengoperasikan serta mengatur sistem komputer[56].

Ketiga elemen sistem komputer tersebut harus saling berhubungan dan membentuk suatu kesatuan. *Hardware* tanpa adanya *software*, maka tidak akan berfungsi seperti apa yang diterapkan, hanya berupa benda mati saja. *Software* yang akan mengoperasikan *hardware*-nya. *Hardware* yang sudah didukung software juga tidak akan berfungsi kalau tidak ada manusianya yang mengoperasikan[57].

---

[54] *Ibid*, hal 4
[55] *Loc.Cit*
[56] *Loc.Cit*
[57] *Loc.Cit*