PERTEMUAN IV

CYBERCRIME

4.1 Pengertian *Cybercrime*

Beberapa pendapat mengidentikkan *cybercrime* dengan computer-crime. ***The U.S. Departement of Justice*** memberikan pengertian computer –crime sebagai *"... any illegal act requering knowledge of computer technology for its perpetration, investigation, or prosecution "* (www.usdoj.gov/criminal/cybercrimes). pengertian tersebut serupa dengan yang diberikan ***Organization Of European Community Development***, yang mendefinisikan computer crime sebagai *"any illegal, unethical or unauthorized behavior relating to the authomatic processing and/or the transsmission of data "*

Adapun **andi hamzah(1989**) dalam tulisanya "aspek – aspek pedana dibidang komputer", mengartikan kejahatan komputer sebagai "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal"

internet sendiri merupakan hasil rekayasa teknologi yang penerapanya bukan hanya menggunakan kecanggihan teknologi komputer, tetapi juga melibatkan teknologi telekomunikasi didalam pengoperasianya. Dari beberapa pengertian diatas dapat dikatakan bahwa *cybercrime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

4.2 Karakteristik *Cybercrime*

Selama ini dalam kejahatan konvensional, kita mengenal ada dua jenis kejahatan, yaitu :

1. **kejahatan kerah biru (blue collar crime**). Kejahatan jenis ini merupakan tindak kriminal yang dilakukan secara konvensional. Para pelakunya digambarkan memiliki steorotip tertentu, misalnya dari golongan kelas sosial bawah, kurang terdidik, penghasilan rendah , contoh kejahatan jenis ini adalah perampokan, pencurian, pembunuhan dll
2. **kejahatan kerah putih (white Collar crime)** kejahatan jenis ini terbagi dalam empat

kelompok yaitu : kejahatan koorporasi, kejahatan birokrat, malpraktik, kejahatan induvidual. Para pelaku biasanya berpendidikan, penghailan tinggi, memegang jabatan terhormat di masyarakat

Cybercrime sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik tersendiri yang berbeda dengan kedua model kejahatan diatas. Karakteristik unik *cybercrime* antara lain :

1. **Ruang lingkup kejahatan**. Sesuai dengan sifat global internet, ruang lingkup kejahatan ini juga bersifat global. *Cybercrime* sering kali dilakukan secara transnasional(melintasi batas antarnegara)
2. **Sifat kejahatan.** Sifat kejahatan di dunia maya yang non – violence, atau tidak menimbulkan kekacauan yang mudah terlihat
3. **Pelaku kejahatan.** Pelaku *cybercrime* bersifat lebih universal meski memiliki ciri khusus yaitu kejahatan dilakukan oleh orang – orang yang menguasai penggunaan internet beserta aplikasinya, pelaku kejahatan tersebut tidak terbatas pada usia dan golongan tertentu, mereka yang sempat tertangkap kabanyakan masih remaja bahkan beberapa diantaranya masih anak – anak.
4. **Modus kejahatan.** Keunikan kejahatan ini adalah penggunaaan teknologi informasi dalam modus operandi, oleh karena itu modus operandi dalam dunia maya tersebut lebih sulit dimengerti oleh orang – orang yang tidak menguasai pengetahuan tentang komputer, teknik pemrograman dan seluk – beluk dunia cyber.
5. **Jenis kerugian yang ditimbulkan.** Kejahatan ini bukan hanya menimbulkan kerugian material maupun non material seperti waktu, nilai, jasa, uang dan harga diri tetapi *Cybercrime* berpotensi menimbulkan kerugian pada banyak bidang seperti politik, sosial bahkan yang lebih besar dampaknya dibandingkan kejahatan berintensitas tinggi lainya. Pada masa mendatang kejahatan semacam ini dapat mengganggu perekonomian nasional yang berbasis teknologi informasi (sistem perbankan, telekomunikasi satelit, jaringan listrik, jaringan lalu lintas penerbangan dll)

4.3 Jenis – jenis Ancaman *(Threats)*

Jenis – jenis ancaman dapat dikelompokan berdasarkan sudut pandang yang berbeda. Berikut ini merupakan jenis-jenis ancaman IT yang dikelompokkan berdasarkan jenis aktivitas, motif kegiatan, dan sasaran kejahatan.

4.3.1 Berdasarkan jenis aktivitasnya

Berdasarkan jenis aktivitas yang dilakukan, *cybercrime* dapat digolongkan menjadi beberapa jenis sebagai berikut :

a. ***Unauthorized Access to Computer System and Service***

Kejahatan yang dilakukan dengan memasuki atau 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 (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi.

Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet, contoh kejahatan ini adalah aktivitas port scanning atau probing yang dilakukan untuk melihat sevis – servis apa saja yang terdapat di server target.

b. ***Illegal Contents***

Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang 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.

c. ***Data Forgery***

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen - dokumen e-commerce dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

d. ***Cyber Espionage, Sabotage and Extortion***

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

Selanjutnya, **sabotage and extortion** merupakan jenis kejahatan yang 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, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

e. ***Offense against Intellectual Property***

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

f. ***Cyberstalking***

Dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet.

g. ***Carding***

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, kehajahatan ini merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdaganan di internet.seperti nomor kartu kredit, nomor PIN ATM

h. ***Penyebaran virus secara sengaja***

Penyebaran virus umumnya dilakukan dengan menggunakan email. Sering kali orang

yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.Contoh kasus: virus bebek, I love you, brontok.

i. *Hacking dan Cracking*

Istilah *hacker* biasanya mengacu pada seseorang yang mempunyai minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya Besarnya minat yang dimiliki seorang hacker dapat mendorongnya untuk memiliki kemampuan penguasaan sistem di atas rata-rata pengguna.Jadi, hacker memiliki konotasi yang netral.

Mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya di sebut cracker. Boleh di bilang para cracker ini sebenarnya adalah hacker yang memanfaatkan kemampuannya untuk hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran.

j. *Cybersquatting and Typosquatting*

Merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. *Typosquatting* adalah kejahatan dengan membuat domain plesetan aitu domain yang mirip dengan nama domain orang lain.

k. *Hijacking*

Merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak)

l. *Cyber Terorism*

Suatu tindakan *cybercrime* termasuk cyber terorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer.

4.3.2 Berdasarkan Motif Kegiatannya

1. Sebagai tindakan murni kriminal

Kejahatan yang murni merupakan tindak kriminal yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah Carding.

2. *Cybercrime* sebagai kejahatan "abu-abu"

Pada jenis kejahatan di internet yang masuk dalam "wilayah abu-abu" cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan, mengingat motif kegiatannya terkadang bukan untuk berbuat kejahatan. Contohnya adalah *probing* atau *portscanning.*

4.3.3 Berdasarkan Sasaran Kejahatannya

1. **Menyerang Individu (Against Person)**

   Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain:

   a. **Pornografi.** Kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas

   b. **Cyberstalking.** Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia maya.

   c. **Cyber-Tresspass.** Kegiatan yang dilakukan melanggar area privasi orang lain. Misalnya *Web Hacking, breaking the PC, Probing, Port Scanning, dsb*

2. **Menyerang Hak Milik (Against Property).**

   Cybercrime yang dilakukan untuk mengganggu atau menyerang hak milik orang lain. Contoh: carding, cybersquatting, typosquatting, hijacking, data forgery

3. **Menyerang Pemerintah (Against Government)**

   Cybercrime Against Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah.

4.4 Penanggulangan *Cybercrime*

Aktivitas pokok *cybercrime* adalah penyerangan terhadap content, sistem komputer dan sistem komunikasi milik orang lain atau milik umum didalam cyberspace. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak harus berinteraksi langsung antara pelaku dengan korban kejahatan, hal ini karena sifat internet yang global. Oleh karena itu semua negara harus mewaspadai perkembangan kejahatan didunia maya tersebut.

Berikut adalah upaya – upaya yang dapat dilakukan untuk menanggulangi merebaknya

kejahatan didunia maya, antara lain :

a. **Pengamanan sistem**. Langkah awal yang harus dilakukan para pengguna teknologi internet adalah mengamankan sistem komputernya, keamanan sistem komputer identik dengan tindakan pencegahan terhadap tindakan – tindakan yang tidak mendapat izin dari pemilik atau sistem komputer
b. **Penanggulangan global.** Bahwa *cybercrime* membutuhkan tindakan global atau internasional untuk menanggulanginya mengingat kejahatan tersebut sering kali bersifat transnasional
c. **Perlunya cyberlaw**. Perkembangan teknologi yang sangat pesat , membutuhkan peraturan dan pengaturan hukum terkait dengan pemanfaatan teknologi tersebut.
d. **Perlunya dukungan lembaga khusus**. Lembaga – lembaga khusus baik milik pemerintah maupun lembaga non – pemerintah sangat diperlukan sebagai upaya penanggulangan *cybercrime*. Di USA terdapat *Computer Crime Intellectual and Property Section (CCIPS)* sebagai divisi khusus dari *USA Departement of Justice*. Sedangkan Indonesia memiliki *Indonesia Computer Emergency Response Team (IDRECT*), sebagai unit yang berfungsi sebagai point of contact bagi orang untuk melaporkan masalah keamanan komputer.

4.5 Contoh Kasus Cyber crime

4.5.1 Luar Negeri

1. 1988. Sendmail dieksploitasi oleh R.T. Morris sehingga melumpuhkan Internet. Diperkirakan kerugian mencapai $100 juta. Morris dihukum denda $10.000.
2. 10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi sebuah airport lokal (Worcester, Mass.) sehingga memutuskan komunikasi di control tower dan menghalau pesawat yang hendal mendarat
3. 7 Februari 2000 s/d 9 Februari 2000. Distributed Denial of Service (Ddos) attack terhadap Yahoo, eBay, CNN, Amazon, ZDNet, E-Trade. Diduga penggunaan program Trinoo, TFN.

4.5.2 Dalam Negeri

1. Dunia perbankan melalui Internet (*ebanking*) Indonesia, dikejutkan oleh ulah seseorang bernama Steven Haryanto, seorang *hacker* dan jurnalis pada majalah Master Web. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan *Internet banking*

Bank Central Asia, (BCA). Steven membeli domain-domain dengan nama mirip www.klikbca.com (situs asli Internet banking BCA), yaitu domain *wwwklik-bca.com, kilkbca.com, clikbca.com, klickca.com.* dan *klikbac.com*.

Isi situs-situs plesetan inipun nyaris sama, kecuali tidak adanya security untuk bertransaksi dan adanya formulir akses (*login form*) palsu. Diperkirakan, 130 nasabah BCA tercuri datanya.

2. Dani Firmansyah, konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta, pada Sabtu 17 April 2004 berhasil melakukan *deface* Pusat Tabulasi Nasional Pemilu http://www.tnp.kpu.go.id milik Komisi Pemilihan Umum (KPU) di Hotel Borobudur Jakarta Pusat dan mengubah nama-nama partai di dalamnya menjadi nama-nama "unik", Hermansyah, pada tanggal 17 April 2004 dengan mengubah nama - nama partai yang ada dengan nama- nama buah dalam website www.kpu.go.id, yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap Pemilu yang sedang berlangsung pada saat itu.
3. Anggota Satuan Cyber Crime Direktorat Kriminal Khusus Kepolisian Daerah Metropolitan Jakarta Raya, Rabu 28 Juli 2004 sekitar pukul 11.15 wib, telah menangkap Johnny Indrawan Yusuf alias Hengky Wiratman alias Irwan Soenaryo asal Malang, Jawa Timur terkait dengan kasus perdagangan VCD porno dan alat bantu seks melalui jaringan internet dalam situs http://www.vcdporno.com

   Menurut perusahaan *Security Clear Commerce* di Texas USA, saat ini Indonesia menduduki peringkat ke 2 setelah Ukraina dalam hal kejahatan *Carding* dengan memanfaatkan teknologi informasi (Internet) yaitu menggunakan nomor kartu kredit orang lain untuk melakukan pemesanan barang secara *online*.