BAB III

KAJIAN TENTANG CYBER CRIME DAN HUBUNGANNYA DENGAN TINDAK PIDANA PENIPUAN

A.**Pengertian dan sejarah Cyber Crime**

Kejahatan komputer atau kejahatan cyber atau kejahatan dunia maya (cybercrime) adalah sebuah bentuk kriminal yang mana menjadikan internet dan komputer sebagai medium melakukan tindakan kriminal.Masalah yang berkaitan dengan kejahatan jenis ini misalnya hacking, pelanggaran hak cipta, pornografi anak, dan eksploitasi anak.Juga termasuk pelanggaran terhadap privasi ketika informasi rahasia hilang atau dicuri, dan lainnya.

Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit, confidence fraud, penipuan identitas, pornografi anak, dll.Walaupun kejahatan dunia maya atau cybercrime umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer

atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.[21]

Kejahatan komputer mencakup berbagai potensi kegiatan ilegal. Umumnya, kejahatan ini dibagi menjadi dua kategori: (1) kejahatan yang menjadikan jaringan komputer dan divais secara langsung menjadi target; (2) Kejahatan yang terfasilitasi jaringan komputer atau divais, dan target utamanya adalah jaringan komputer independen atau divais.Contoh kejahatan yang target utamanya adalah jaringan komputer atau divais yaitu:

1) Malware (malicious software / code)

Malware (berasal dari singkatan kata malicious dan software) adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, server atau jaringan komputer tanpa izin (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 computer" terkadang dipakai sebagai frasa pemikat (catch phrase) untuk mencakup semua jenis perangkat perusak, termasuk virus murni (true virus).

2) Denial-of-service (DOS) attacks

Denial of service attack atau serangan DoS adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai

[21]http://dutaxp.blogspot.com/2012/06/pengertian-dan-jenis-jenis-cybercrime.html 20/6/2014 pukul 21:00

komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

3) Computer viruses

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 murni hanya dapat menyebar dari sebuah komputer ke komputer lainnya (dalam sebuah bentuk kode yang bisa dieksekusi).ketika inangnya diambil ke komputer target, contohnya ketika user mengirimnya melalui jaringan atau internet, atau membawanya dengan media lepas (floppy disk, cd, dvd, atau usb drive). Virus bisa bertambah dengan menyebar ke komputer lain dengan mnginfeksi file pada network file system (sistem file jaringan) atau sistem file yang diakses oleh komputer lain.

Contoh kejahatan yang menjadikan jaringan komputer atau divais sebagai alat yaitu:

1) *Cyber stalking* (Pencurian dunia maya)

Cyberstalking adalah penggunaan internet atau alat elektronik lainnya untuk menghina atau melecehkan seseorang, sekelompok orang, atau organisasi.Hal ini termasuk tuduhan palsu, memata-matai, membuat ancaman, pencurian identitas, pengerusakan data atau peralatan, penghasutan anak di bawah umur untuk seks, atau mengumpulkan informasi untuk mengganggu. Definisi dari "pelecehan"

harus memenuhi kriteria bahwa seseorang secara wajar, dalam kepemilikan informasi yang sama, akan menganggap itu cukup untuk menyebabkan kesulitan orang lain secara masuk akal.[22]

2) Penipuan dan pencurian identitas

Pencurian identitas adalah menggunakan identitas orang lain seperti KTP, SIM, atau paspor untuk kepentingan pribadinya, dan biasanya digunakan untuk tujuan penipuan. Umumnya penipuan ini berhubungan dengan Internet, namun sering huga terjadi di kehidupan sehari-hari. Misalnya penggunaan data yang ada dalam kartu identitas orang lain untuk melakukan suatu kejahatan. Pencuri identitas dapat menggunakan identitas orang lain untuk suatu transaksi atau kegiatan, sehingga pemilik identitas yang aslilah yang kemudian dianggap melakukan kegiatan atau transaksi tersebut.

3) Phishing scam

Dalam sekuriti komputer, phising (Indonesia: pengelabuan) adalah suatu bentuk penipuan yang dicirikan dengan percobaan untuk mendapatkan informasi peka, seperti kata sandi dan kartu kredit, dengan menyamar sebagai orang atau bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti surat elektronik atau pesan instan. Istilah phishing dalam bahasa Inggris berasal dari kata *fishing* (= memancing), dalam hal ini berarti memancing informasi keuangan dan kata sandi pengguna.[23]

[22] http://id.wikipedia.org/wiki/Cyberstalking 22/6/2014 diakses pukul 22:00
[23] metadatastudio.com/pengertian-email-phishing 22/6/2014 diakses pukul 22:00

4) **Perang informasi *(Information warfare)***

Perang Informasi adalah penggunaan dan pengelolaan informasi dalam mengejar keunggulan kompetitif atas lawan.perang Informasi dapat melibatkan pengumpulan informasi taktis, jaminan bahwa informasi sendiri adalah sah, penyebaran propaganda atau disinformasi untuk menurunkan moral musuh dan masyarakat, merusak kualitas yang menentang kekuatan informasi dan penolakan peluang pengumpulan-informasi untuk menentang kekuatan. Informasi perang berhubungan erat dengan perang psikologis.

Contohnya ketika seseorang mencuri informasi dari situs, atau menyebabkan kerusakan computer atau jaringan komputer.Semua tindakan ini adalah virtual (tidak nyata) terhadap informasi tersebut –hanya ada dalam dunia digital, dan kerusakannya –dalam kenyataan, tidak ada kerusakan fisik nyata kecuali hanya fungsi mesin yang bermasalah.Komputer dapat dijadikan sumber bukti. Bahkan ketika komputer tidak secara langsung digunakan untuk kegiatan kriminal, komputer merupakan alat yang sempurna untuk menjaga record atau catatan, khususnya ketika diberikan tenaga untuk mengenkripsi data. Jika bukti ini bisa diambil dan didekripsi, ini bisa menjadi nilai bagi para investigator criminal.[24]

5) **Sejarah *Cyber Crime***

Sejarah *Cyber Crime*Awal mula penyerangan didunia *Cyber* pada tahun 1988 yang lebih dikenal dengan istilah *Cyber Attack*.Pada saat itu ada seorang mahasiswa yang berhasil menciptakan sebuah worm atau virus yang menyerang program computer dan mematikan sekitar 10% dari seluruh jumlah komputer di

[24] http://www.lemhannas.go.id/portal/daftar-artikel/1556-cyber-warfare.html diakses 22/6/2014 pukul 22:00

dunia yang terhubung ke internet Pada tahun 1994 seorang anak sekolah musik yang berusia 16 tahun yang bernama RichardPryce, atau yang lebih dikenal sebagai "*the hacker*" alias "*Datastream Cowboy*"(liran data cowboy), ditahan lantaran masuk secara ilegal ke dalam ratusan sistem komputer rahasia termasuk pusat data dari *Griffits AirForce*, *NASA*(National Aeronautics and Space Administration) dan Korean Atomic Research Institute atau badan penelitian atom Korea Dalam interogasinya dengan FBI, ia mengaku belajar hacking dan cracking dari seseorang yang dikenalnya lewat internet dan menjadikannya seorang mentor, yang memiliki julukan "Kuji".Hebatnya, hingga saat ini sang mentor pun tidak pernah diketahui keberadaannya.Hingga akhirnya, pada bulan Februari 1995, giliran Kevin Mitnick diganjar hukuman penjara untukyang kedua kalinya. Dia dituntut dengan tuduhan telah mencuri sekitar 20.000 nomor kartu kredit!Bahkan, ketika ia bebas, ia menceritakan kondisinya di penjara yang tidak boleh menyentuh komputer atau telepon.

B.**Jenis-Jenis Tindak Pidana yang dilakukan dengan Cyber Crime**

Dalam perembangannya tindak pidana *Cyber Crime* memiliki berbagai jenis modus yang dilakukan dan sering terjadi pada dunia maya:

a. Unauthorized Access to Computer System and Service

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatusistem 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.Kita tentu belum lupa ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website milik pemerintah RI dirusak oleh hacker (Kompas, 11/08/1999). Beberapa waktu lalu, hacker juga telah berhasil menembus masuk ke dalam data base berisi data para pengguna jasa America Online (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang ecommerce yang memiliki tingkat kerahasiaan tinggi (Indonesian Observer, 26/06/2000). Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para hacker, yang mengakibatkan tidak berfungsinya situs ini beberapa waktu lamanya.

b. *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.Dapat kita contohkan saat ini.Situs mesin pencari bing milik microsoft yang konon di tuduh menyerupai sebuah situs milik perusahaan travel online.

c. 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 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.Masih ingat dengan kasus prita mulyasari yang sampai saat ini belum selesai.Hanya gara-gara tulisan emailnya yang sedikit merusak nama baik sebuah institusi kesehatan swasta dia di seret ke meja hijau.

d. Cyberstalking

Kejahatan jenis ini 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. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya. Contoh Kasus : Misalnya e-mail yang berisi ajakan bergabung dengan suatu website, email yang berisi ajakan untuk membeli produk tertentu, mail yang berisi kontes / undian berhadiah. Undang-undang ITE Pasal 25: Penggunaan setiap informasi melalui media elektronik yang menyangkut data tentang hak pribadi seseorang harus dilakukan atas persetujuan dari orang yang bersangkutan, kecuali ditentukan lain oleh peraturan perundang-undangan.

e. Hacking dan Cracker

Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di

internet lazimnya disebut cracker.Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-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. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan. Contoh Kasus : Pada tahun 1983, pertama kalinya FBI menangkap kelompok kriminal komputer The 414s(414 merupakan kode area lokal mereka) yang berbasis di Milwaukee AS. Kelompok yang kemudian disebut hacker tersebut melakukan pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos.Salah seorang dari antara pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan. Undang-Undang Pasal 27 (1) Setiap orang dilarang menggunakan dan atau mengakses komputer dan atau sistem elektronik dengan cara apapun tanpa hak, untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan atau sistem elektronik. (Pidana empat tahun penjara dan denda Rp 1 miliar).

f. Cybersquatting and Typosquatting

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan

nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan. Contoh Kasus : Contoh kasus yang beredar di international adalah kasus Yahoo yang menuntut OnlineNIC atas aksi cybersquatting pada 500 nama domain yang mirip atau dapat membingungkan para penggunanya termasuk yahoozone.com, yahooyahooligans.com dan denverwifesexyahoo.com. Undang-Undang : Pasal 23 (2): Pemilikan dan penggunaan nama domain sebagaimana dimaksud dalam ayat (1) wajib didasarkan pada itikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak orang lain. (Tindak pidana sebagaimana dimaksud dalam ayat (1) hanya dapat dituntut atas pengaduan dari orang yang terkena tindak pidana) (Pidana enam bulan atau denda Rp 100 juta).

g. Arp spoofing

Arp spoofing adalah teknik yang cukup populer untuk melakukan penyadapan data, terutama data username/password yang ada di jaringan internal. Intinya adalah dengan mengirimkan paket ARP Reply palsu sehingga merubah data MAC Address:IP yang ada di tabel ARP komputer target. Perubahan data ini menyebabkan pengiriman paket TCP/IP akan melalui attacker sehingga proses penyadapan dapat dilakukan.

h. Carding

Adalah berbelanja mengunakan nomor atau identitas kartu kredit orang lain yang dilakukan secara ilegal. Pelakunya biasa disebut carder. Parahnya indonesia menduduki peringkat kedua dunia setelah Ukraina untuk kasus ini. Tak tanggung-tanggung 20% transaksi internet dari Indonesia adalah dari hasil Carding.Itulah

sebabnya banyak situs belanja online yang memblokir ip asal Indonesia. Atau dengan kata lain konsumen Indonesia tidak boleh belanja di situs tersebut. Perkembangan terakhir pelaku carding juga mulai menyusup ke ruang-ruang chat seperti mIRC dengan mengiming-imingi barang berharga "miring", begitu ada yang tertarik si pembeli disuruh membayar via rekening. Begitu uang terkirim barang tak pernah dikirim. Sebagai tambahan, kadang sebagian orang menganggap pelaku carding sama dengan hacker. Hal ini jelas tidak benar karena untuk melakukan carding tidak terlalu memerlukan otak.Mereka cukup mengetahui nomor kartu dan tanggal kadaluwarsa.Sedangkan hacker adalah orang yang sangat paham betul mengenai sistem keamanan suatu jaringan dan memerlukan waktu yang tidak sebentar untuk menjadi seorang hacker sejati.

i. *Defacing*

Defacing adalah kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs Menkominfo dan Partai Golkar, BI baru-baru ini dan situs KPU saat pemilu 2004 lalu. Tindakan deface ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang jahat, untuk mencuri data dan dijual kepada pihak lain.

j. Phising

Phising adalah tindak kejahatan memancing pemakai komputer di internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password

yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya.

k. Spamming

Adalah mengirimkan pesan atau iklan yang tidak dikehendaki melalui surat elektronik (E-mail). Pengiriman e-mail dapat hadiah, lotere, atau seseorang yang mengaku mempunyai rekening di Amerika, baghdad dan sebagainya lalu meminta tolong untuk mencairkan. Belakangan ini seorang spammer telah ditangkap dan terancam menghadapi bui karena aksinya yang menyalahi aturan koneksi Facebook.Perkara tersebut telah ditangani oleh Kejaksaan Agung Amerika Serikat. Sanford Wallace atau yang dikenal dengan nama "Spam King" berhasil digiring oleh Jeremy Fogel, hakim U.S Distric Court for Northern Distric of California atas kasus mail marketing. Jaksa Agung tersebut akan memprosesnya atas tuduhan pencemaran dalam akses Facebook. Dan hasilnya Wallace dikenai sanksi membayar denda sebesar US$ 230 juta.Yang saya pertanyakan apakah inbox berantai di Facebook juga termasuk kejahatan di internet dan bisa di kenai pasal pidana?Soalnya akhir-akhir ini inbox di Akun Facebook saya sering mendapat pesan berantai yang tidak berkesudahan.

l. Malware

Adalah program komputer yang mencari kelemahan dari suatu software.Umumnya malware diciptakan untuk membobol atau merusak suatu software atau operating system. Malware terdiri dari berbagai macam, yaitu: virus, worm, trojan horse, adware, browser hijacker, dll. Di pasaran alat-alat komputer dan toko perangkat lunak (software) memang telah tersedia antispam dan anti

virus, dan anti malware.Meski demikian, bagi yang tak waspadai selalu ada yang kena.Karena pembuat virus dan malware umumnya terus kreatif dan produktif dalam membuat program untuk mengerjai korban-korbannya.

m. Jamming

Jamming adalah sebuah bentuk interferensi dengan mengurangi energi frekuensi radio dari sumber energi tertentu dengan karakteristik tertentu untuk mencegah receiver menerima sinyal GPS pada suatu area yang ditargetkan.Karakteristik Sinyal GPS berada bebas diangkasa membuat orang bisa dengan mudah untuk membuat tipuan sinyal sejenis.Hanya dengan sebuah sinyal generator maka frekuensi radio dari oscillator dapat dimodifikasi.Bahkan hal ini bisa dilakukan dengan menggunakan sebuah pesawat Hand Phone. Biasanya para jammer jika takut diketahui didarat umumnya akan melakukannya dari atas pesawat udara atau balon udara.

n. .Spoofing

adalah sebuah teknik yang telah lama digunakan untuk mengelabui wilayah jangkauan operasi radar. Pada kasus GPS, tujuan dari teknik ini adalah untuk membuat receiver aktif GPS terkunci pada sebuah sinyal palsu, dan kemudian secara perlahan – lahan dibelokan menuju target yang lain.Meaconing adalah reception, delay dan rebroadcast dari radio navigasi yang bertujuan untuk mengelabui sistem navigasi atau penggun

o. 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-data pentingnya tersimpan dalam suatu sistem yang computerized.Biasaynya si penyerang menyusupkan sebuah program mata-mata yang dapat kita sebut sebagai spyware.

p. 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.

q. Data Forgery

Merupakan 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 seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.

r. Cyber Sabotage and Extortion

Merupakan kejahatan yang paling mengenaskan.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, 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. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu.Kejahatan ini sering disebut sebagai cyber-terrorism.

s. 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 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.Masih ingat dengan kasus prita mulyasari yang sampai saat ini belum selesai.Hanya gara-gara tulisan emailnya yang sedikit merusak nama baik sebuah institusi kesehatan swasta dia di seret ke meja hijau.

t. Snifing

adalah kegiatan menyadap dan/atau menginspeksi paket data menggunakan sniffer software atau hardware di internet. Kegiatan ini sering disebut sebagai serangan sekuriti pasif dengan cara membaca data yang berkeliaran di internet, dan memfilter khusus untuk host tujuan tertentu. Jadi kegiatan ini tidak melakukan apa-apa terhadap data, tidak merubah dan tidak memanipulasi.Cukup menyadap.Ia digunakan untuk mendapatkan informasi seperti password, data-data rahasia dan lainnya. Sering digunakan para analyst networking, baik dari kalangan developer maupun network administrator, untuk melakukan troubleshooting.

u. Spoofing

Spoofingadalah aksi pemalsuan identitas. IP Spoofing merupakan tehnik yang digunakan bagi penyelundup untuk mengakses sebuah network dengan mengirimkan paket/pesan dari sebuah komputer yang mengindikasikan bahwa paket/pesan tersebut berasal dari host yang terpercaya. Untuk melakukan aksi ini para penyelundup menggunakan tehnik yang bermacam-macam, dan spoofing sendiri merupakan salah satu bagian dari proses penyerangan.[25]

C. **Perbandingan Kajian Hukum Terhadap Tindak Pidana Penipuan Melalui Cyber Crime menurut Undang-Undang no 11 tahun 2008 dengan KUHP pasal 378**

[25]http://vertikalpoint.blogspot.com/2012/10/jenis-jenis-cyber-crime.html diakses 22/6/2014 pukul 22:00

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") tidak secara khusus mengatur mengenai tindak pidana penipuan. Selama ini, tindak pidana penipuan sendiri diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana ("KUHP"), dengan rumusan pasal sebagai berikut: "Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat (*hoedaningheid*) palsu; dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam, karena penipuan, dengan pidana penjara paling lama empat tahun."

Walaupun UU ITE tidak secara khusus mengatur mengenai tindak pidana penipuan, namun terkait dengan timbulnya kerugian konsumen dalam transaksi elektronik terdapat ketentuan Pasal 28 ayat (1) UU ITE yang menyatakan: "Setiap Orang dengan sengaja, dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

Terhadap pelanggaran Pasal 28 ayat (1) UU ITE diancam pidana penjara paling lama enam tahun dan/atau denda paling banyak Rp1 miliar, sesuai pengaturan Pasal 45 ayat (2) UU ITE.

Jadi, dari rumusan-rumusan Pasal 28 ayat (1) UU ITE dan Pasal 378 KUHP tersebut dapat kita ketahui bahwa keduanya mengatur hal yang berbeda. Pasal 378 KUHP mengatur penipuan (penjelasan mengenai unsur-unsur dalam Pasal 378 KUHP sementara Pasal 28 ayat (1) UU ITE mengatur mengenai berita bohong

yang menyebabkan kerugian konsumen dalam transaksi elektronik (penjelasan mengenai unsur-unsur dalam Pasal 28 ayat (1) UU ITE .Walaupun begitu, kedua tindak pidana tersebut memiliki suatu kesamaan, yaitu dapat mengakibatkan kerugian bagi orang lain. Tapi, rumusan Pasal 28 ayat (1) UU ITE tidak mensyaratkan adanya unsur "menguntungkan diri sendiri atau orang lain" sebagaimana diatur dalam Pasal 378 KUHP tentang penipuan.

Pada akhirnya, dibutuhkan kejelian pihak penyidik kepolisian untuk menentukan kapan harus menggunakan Pasal 378 KUHP dan kapan harus menggunakan ketentuan-ketentuan dalam Pasal 28 ayat (1) UU ITE. Namun, pada praktiknya pihak kepolisian dapat mengenakan pasal-pasal berlapis terhadap suatu tindak pidana yang memenuhi unsur-unsur tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP dan memenuhi unsur-unsur tindak pidana Pasal 28 ayat (1) UU ITE. Artinya, bila memang unsur-unsur tindak pidananya terpenuhi, polisi dapat menggunakan kedua pasal tersebut.

D. Faktor-Faktor yang mempengaruhi tindak pidana Cyber Crime

Era kemajuan teknologi informasi ditandai dengan meningkatnya penggunaan internet dalam setiap aspek kehidupan manusia. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, di sisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan tindak pidana.

Faktor-faktor yang mempengaruhi cyber crime adalah :

1. Faktor Politik.

Mencermati maraknya cyber crime yang terjadi di Indonesia dengan permasalahan yang dihadapi oleh aparat penegak, proses kriminalisasi di bidang cyber yang terjadi merugikan masyarakat.Penyebaran virus koputer dapat merusak jaringan komputer yang digunakan oleh pemerintah, perbankan, pelaku usaha maupun perorangan yang dapat berdampak terhadap kekacauan dalam sistem jaringan. Dapat dipastikan apabila sistem jaringan komputer perbankan tidak berfungsi dalam satu hari saja akan mengakibatkan kekacauan dalam transaksi perbankan.

Kondisi ini memerlukan kebijakan politik pemerintah Indonesia untuk menanggulangi cyber crime yang berkembang di Indonesia.Aparat penegak hukum telah berupaya keras untuk menindak setiap pelaku cyber crime, tapi penegakkan hukum tidak dapt berjalan maksimal sesuai harapan masyarakat karena perangkat hukum yang mengatur khusus tentang cyber crime belum ada.

Untuk menghindari kerugian yang lebih besar akibat tindakan pelaku cyber crime maka diperlukan kebijakan politik pemerintah Indonesia untuk menyiapkan perangkat hukum khusus (lex specialist) bagi cyber crime.Dengan perangkat hukum ini aparat penegak hukum tidak ragu-ragu lagi dalam melakukan penegakan hukum terhadap cyber crime.

2. Faktor Ekonomi.

Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang-barang produksi.Jaringan komputer dan internet merupakan media yang sangat murah untuk promosi.Masyarakat dunia banyak yang menggunakan media ini untuk mencari barang-barang kepentingan perorangan maupun korporasi.Produk barang yang dihasilkan oleh indutri di Indonesia sangat banyak dan digemari oleh komunitas Internasional.Para pelaku bisnis harus mampu memanfaatkan sarana internet dimaksud.Krisis ekonomi yang melanda bangsa Indonesia harus dijadikan pelajaran bagi masyarakat Indonesia untuk bangkit dari krisis dimaksud.Seluruh komponen bangsa Indonesia harus berpartisipasi mendukung pemulihan ekonomi.Media internet dan jaringan komputer merupakan salah satu media yang dapat dimanfaatkan oleh seluruh masyarakat untuk mempromosikan Indonesia.

3. Faktor Sosial Budaya.

Faktor sosial budaya dapat dilihat dari beberapa aspek, yaitu :

Kemajuan teknologi Informasi Dengan teknologi informasi manusia dapat melakukan akses perkembangan lingkungan secara akurat, karena di situlah

terdapat kebebasan yang seimbang, bahkan dapat mengaktualisasikan dirinya agar dapat dikenali oleh lingkungannya.

Sumber Daya Manusia.

Sumber daya manusia dalam teknologi informasi mempunyai peranan penting sebagai pengendali sebuah alat.Teknologi dapat dimanfaatkan untuk kemakmuran namun dapat juga untuk perbuatan yang mengakibatkan petaka akibat dari penyimpangan dan penyalahgunaan.Di Indonesia Sumber Daya Pengelola teknologi Informasi cukup, namun Sumber Daya untuk memproduksi masih kurang.Hal ini akibat kurangnya tenaga peneliti dan kurangnya biaya penelitian dan apresiasi terhadap penelitian.Sehingga Sumber Daya Manusia di Indonesia hanya menjadi pengguna saja dan jumlahnya cukup banyak.

Komunitas Baru.

Dengan adanya teknologi sebagai sarana untuk mencapai tujuan, di antaranya media internet sebagai wahana untuk berkomunikasi, secara sosiologis terbentuk sebuah komunitas baru di dunia maya. Komunitas ini menjadim populasi gaya baru yang cukup diperhitungkan. Pengetahuan dapat diperoleh dengan cepat. [26]

[26] http://dumadia.wordpress.com/2009/04/02/aplikasi-konvensi-cyber-crime-2001-dalam-uu-no-11-tahun-2008-mengenai-informasi-dan-transaksi-elektronik-ite"20/6/2014 pukul 21:00