Jurnal Bisnis dan Ekonomi (JBE), September 2011, Hal. 185 – 195 **Vol. 18, No. 2 185**
ISSN: 1412-3126

KASUS *CYBERCRIME* DI INDONESIA
Indonesia's *Cybercrime Case*

Dista Amalia Arifah
Program Studi Manajemen, Fakultas Ekonomi UNISSULA
Jl. Kaligawe Km. 4, Semarang
(distaamalia@gmail.com)

ABSTRAK

Pada saat awal ditemukan, komputer hanyalah sebuah mesin besar dengan kemampuan yang terbatas. Tetapi setelah mengalami perkembangan dan pemutakhiran dalam waktu yang relatif singkat, komputer menjadi sebuah mesin popular dengan banyak kemampuan, orang menjadi tertarik dan mengalami ketergantungan dengan komputer. Apalagi setelah internet ditemukan. Perkembangan komputer menjadi semakin pesat dalam waktu yang relatif singkat. Ada banyak keunggulan internet, begitu dengan pula bahaya yang diakibatkan oleh internet, kejahatan melalui internet atau yang lebih dikenal dengan Cybercrime, bermacam-macam jenisnya seperti; virus, penolakan akses dan sebagainya. Kerusakan yang disebabkan oleh Cybercrime sudah tak terhitung lagi tetapi hukum yang secara khusus menangani Cybercrime di Indonesia belum sepenuhnya berjalan. Beberapa pasal Kitab Undang-undang Hukum Pidana (KUHP) dapat digunakan untuk menjerat pelaku kejahatan yang berhubungan dengan komputer atau internet, meskipun tidak dapat berlaku untuk semua jenis kejahatan Cybercrime yang ada.Hambatan bagi proses penyidikan Cybercrime terkait dengan Undang-undang, kemampuan perangkat hukum, alat bukti dan fasilitas pendukungnya. Langkah-langkah yang dapat diambil untuk menyelesaikan masalah penyidikan Cybercrime antara lain; menyempurnakan undang-undang tentang Cybercrime, melakukan training Cybercrime pada penegak hukum secara berkelanjutan dan membangun divisi khusus penyidikan Cybercrime yang lengkap serta menggalakkan dan mensosialisasikan pencegahan Cybercrime secara luas.

Kata kunci: Komputer, Internet, Cybercrime, Hacker, tindakan hukum

ABSTRACT

At the beginning was found, Computer is a huge machine with limited ability, but in recent years after many upgrade and update Computer become a popular machine which many ability, men become amused and addict with It. Moreover when internet was invented, Computer development going rapidly than years. There are so much Internet advantage,otherwise threatened by danger, Crime over Internet or known with Cybercrime, which are take many form through; virus, denial of service etc. Damage caused by Cybercrime was uncountable anymore but specific law related to Cybercrime in Indonesia wasn't ready yet. Any article found in inner part and outer part of Indonesian Criminal Code (KUHP) can be used to the crime related computer or Internet but not to all kinds. The barrier of Cybercrime investigation process connect to the rules, law officer ability, evidence and supporting facilities. Some problem solving to overcome Cybercrime investigation should be taken like: completing Cybercrime rules, hold Cybercrime training continuosly for law officer and build specific Cybercrime investigation division also campaign Cybercrime prevention widely among citizen.

***Key words** : computer, Internet, Cybercrime, Hacker, law action*

PENDAHULUAN

Saat pertama kali ditemukan komputer hanyalah sebuah mesin besar dengan kemampuan yang terbatas, dalam waktu yang singkat piranti tersebut telah mengalami perkembangan yang signifikan baik dari sisi kemampuan maupun ukuran. Banyak perusahaan menggunakan komputer dalam aktivitas hariannya, begitu pula dengan pemakai perseorangan. Terlebih lagi sejak ditemukannya internet pada tahun 1969 dan mengalami booming seperempat abad kemudian.

Internet telah memberikan dampak yang jauh lebih besar pada komun
daripada p[illegible]mbangan

pula dilakukannya transaksi bisnis via Internet. Perusahaan-perusahaan berskala dunia semakin banyak memanfaatkan fasilitas internet. Sementara itu tumbuh transaksi-transaksi melalui elektronik atau on-line dari berbagai sektor, yang kemudian memunculkan istilah; *e-banking*, *e-commerce*, *e-trade*, *e-business*, *e-government*, *e-education* dan *e-retailing*. Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif.

Tentunya untuk yang bersifat positif kita semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi ini. Tidak dapat dipungkiri bahwa teknologi Internet juga membawa dampak negatif yang tidak kalah banyaknya dengan manfaat yang ada. Internet membuat kejahatan yang semula bersifat konvensional berkembang menjadi sebuah kejahatan modern dengan tingkat kerugian yang lebih besar dengan dampak yang luas. Contohnya; adanya tindak pidana via *e-commerce* oleh sekelompok pemuda di Medan, hacker Steven Haryanto dan Dani Hermansyah yang mengacaukan website entitas tertentu, beberapa artis yang dicemarkan namanya melalui sebuah situs prostitusi. Banyaknya dampak negatif yang timbul dan berkembang melahirkan pendapat bahwa tidak ada komputer yang aman kecuali dipendam dalam tanah sedalam 100 meter dan tidak memiliki hubungan apapun juga.

Hilangnya batas ruang dan waktu di Internet mengubah banyak hal. Perkembangan yang pesat dalam pemanfaatan jasa internet pada akhirnya mengundang terjadinya kejahatan, yang lebih dikenal dengan nama Cybercrime. C*ybercrime* merupakan perkembangan dari *computer crime.* Indonesia sebagai salah satu negara dengan penduduk terpadat didunia juga tidak lepas dari persoalan tersebut. Indonesia menyumbang 2,4% kejahatan *cyber* di dunia. Angka ini naik 1,7% dibanding tahun 2010 lalu di mana Indonesia menempati peringkat 28. Hal ini tak lain disebabkan oleh terus meningkatnya jumlah pengguna internet di Indonesia (Kompas, 16 Mei 2012).

Terlebih, sekarang Indonesia masuk lima besar pengguna jejaring sosial terbanyak di dunia, disinyalir penjahat *cyber* lebih mudah lagi dalam menjalankan aksinya. Para penjahat *cyber* memanfaatkan jaringan pertemanan melalui jejaring sosial, karena sebagian besar pengguna jejaring sosial percaya begitu saja atas *link* atau konten yang mereka terima dari sesama teman. Tanpa melakukan konfirmasi atau pengecekan lebih lanjut pengguna jejaring sosial tersebut melakukan akses langsung ke web atau situs yang mereka terima, yang tanpa disadari berisi program jahat. (Kompas, 16 Mei 2012).

Hukum yang salah satu fungsinya menjamin kelancaran proses pembangunan nasional sekaligus mengamankan hasil-hasil yang telah dicapai harus dapat melindungi hak para pemakai jasa internet sekaligus menindak tegas para pelaku *Cybercrime*. Melihat dari sifatnya *Cybercrime* termasuk dalam kategori *borderless cryme* (kejahatan tanpa batasan ruang dan waktu), *sehingga* dalam memberantas tindak kejahatan *Cybercrime*, diperlukan langkah-langkah yang kompleks, terintegrasi serta berkesinambungan dari banyak pihak, tidak hanya tugas penegak hukum semata.

Definisi Cybercrime

Untuk memudahkan pemahaman, berikut beberapa pendapat tentang apa yang dimaksud dengan *Cybercrime*. Menurut Gregory (2005) *Cybercrime* adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengekploitasi komputer lain yang terhubung dengan internet juga. Adanya lubang-lubang keamanan pada sistem operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para *hacker, cracker* dan *script kiddies* untuk menyusup ke dalam komputer tersebut.

Sedangkan menurut Kepolisian Inggris Tahir (2009) ”*Cyber Crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital”. Menurut Tavani (Fajri, 2008) definisi *Cybercrime*, yaitu ”kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber*”. Beberapa definisi lain seperti yang terangkum dalam artikel Golose (2006) antara lain menurut The U.S. [illegible] memberikan pengerti[illegible] sebagai:".

Computer technology for its perpetration, investigation, or prosecution". Pengertian lainnya diberikan oleh Organization of European Community Development, yaitu: "*any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data*". Andi Hamzah mengartikan C*ybercrime* sebagai kejahatan di bidang komputer secara umum sebagai penggunaan komputer secara ilegal.

Dari beberapa pengertian di atas, *cybercrime* dapat dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana / alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Kejahatan komputer yang diasosiasikan dengan *hacker*, biasanya menimbulkan arti yang negatif. Himanen menyatakan bahwa *hacker* adalah seseorang yang senang memprogram dan percaya bahwa berbagi informasi adalah hal yang sangat berharga, dan *hacker* adalah orang pintar dan senang terhadap semua (Fajri, 2008). Banyak diantara *hacker* adalah pegawai sebuah perusahaan yang loyal dan dipercaya oleh perusahaan-nya, dan dia tidak perlu melakukan kejahatan computer. Mereka adalah orang-orang yang tergoda pada lubang-lubang yang terdapat pada sistem computer. Sehingga kesempatan merupakan penyebab utama orang-orang tersebut menjadi 'penjahat cyber.

Istilah yang lain yaitu *cracker*, *hacker* tidaklah sama seperti *cracker*. *Hacker Jargon File* (Fajri, 2008) menyatakan bahwa *cracker* adalah orang yang merusak sistem keamanan, *cracker* biasanya kemudian melakukan 'pencurian' dan tindakan anarki, begitu mereka mendapat akses. Sehingga muncul istilah *whitehat* dan *blackhat*. Whitehat adalah *hacker* yang lugu, dan blackhat adalah seperti yang disebutkan di atas sebagai *cracker*, namun demikian, orang lebih senang menyebutkan *hacker* untuk *whitehat* dan *blackhat*, walaupun pengertiannya berbeda.

Sasaran dan Teknik pelaku Cybercrime

Biasanya *hacker* menggunakan *tool-tool* yang sudah ada di internet. *Tool* tersebut kemudian dijalankan untuk menyerang sistem computer. *Hacker* berpengalaman membuat *script* atau program sendiri untuk melakukan *hacking*, yang menjadi incaran sasaran yaitu :

- Database kartu kredit
- Database account bank
- Database informasi pelanggan
- Pembelian barang dengan kartu kredit palsu atau kartu credit orang lain yang bukan merupakan hak kita (carding)
- Mengacaukan sistem

Hacker tersebut dapat menjalankan aksinya melalui Internet Relay Chat (IRC), Voice over IP (VoIP), ICQ, Online forums, dan Encryption. Dalam menjalankan aksinya hacker menggunakan tahapan sebagai berikut (Gregory, 2005):

a. *Footprinting*

Suatu tahap mencari informasi secara umum terhadap target *Scanning* pada tahap ini merupakan tahap pencarian terhadap lubang untuk masuk ke sistem

b. *Enumeration*

Telaah intensif terhadap sistem, mencari *user account* yang absah, resource jaringan dan aplikasi yang sedang berjalan pada sistem.

c. *Gaining Access*

Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password, *serta melakukan buffer overflow.*

f. Escalating Privilege

Bila baru mendapatkan user password di tahap sebelumnya, di tahap ini diusahakan mendapat privilese admin jaringan dengan password cracking atau melakukan eksploitasi.

g. *Pilfering*

Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup *evaluasi trust* dan pencarian cleartext password di registry, config file, dan user data.

h. *Covering Tracks*

Begitu kontrol penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan *network log* dan penggunaan *hide tool* seperti maca *streami*

i. *Creating Backdoors*

Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk *user account* palsu, menjadwalkan *batch job*, mengubah *startup file*, menanamkan servis pengendali jarak jauh serta *monitoring system.*

j. *Denial of Service*

Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Dengan membanjiri system target meliputi SYN flood, teknik-teknik ICMP, Supernuke, land/latierra, teardrop, bonk, newtear, trinoo, smurf, dan lain-lain

Dengan metodologi seperti ini, *hacker* melakukan penyerangan dengan berbagai tehnik seperti *exploit* (eksploitasi langsung ke sistem), *spoofing* (penyamaran), *sniffing* penangkapan data/capture data), dan *social engineering* (rekayasa sosial).

Jenis dan Penggolongan *Cybercrime*

Begitu banyaknya peristiwa kejahatan melalui dunia virtual (internet) sehingga menyulitkan orang awam untuk memahami apa sebenarnya yang dimaksud dengan *Cybercrime*, bagaimana cara untuk mengatasi dan mencegahnya. Cybercrime mempunyai jenis yang amat beragam dan semakin berkembang dari hari ke hari. (Lampiran 1)

Kejahatan melalui Internet dibagi menjadi;

a. Kejahatan Dunia Virtual *(Cybercrime)* ;

Kejahatan tersebut hanya bisa terjadi dengan menggunakan perangkat komputer, melalui jaringan komputer, akses serta terjadi di dunia virtual begitu juga dengan sasaran kejahatan.

1. *Cyberpiracy* → penggunaan teknologi komputer untuk mencetak ulang software atau informasi; mendistribusikan informasi atau software tersebut melalui jaringan komputer. Contoh Kasus : Mendistribusikan mp3 di internet melalui teknologi peer to peer
2. *Cybertrespass* → penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer sebuah organisasi atau individu; Web site yang di-*protect* dengan password.

   Contoh Kasus: Melakukan serangan DoS *(deniel of Service)* ke sebuah web
3. *Cybervandalism* → penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi informasi elektronik; menghancurkan data di computer.

Contoh Kasus :

i. Melakukan serangan DoS *(deniel of Service)* ke sebuah web

ii. Membuat virus SASSER

b. Perbedaan antara Cybercrime dengan Kejahatan yang berhubungan dengan Dunia Virtual *(Cyber Related Crime)* ;

Banyak kejahatan yang menggunakan teknologi komputer tidak bisa disebut *cybercrime*. Pedophilia, stalking, dan pornografi bisa disebarkan dengan atau tanpa menggunakan *cybertechnology*, sehingga tidak bisa disebut *cybercrime*, tetapi masuk dalam kategori *cyber-related crime. Cyber-related crime* dikelompokkan menjadi :1.

1. *Cyber-assisted crime* → komputer membantu pelaku melakukan kejahatan biasa dan tidak berhubungan dengan komputer.

   Contoh kasus: Penggunaan komputer untuk menggelapkan pajak.
2. *Cyber-exacerbated crime* → cyber-teknologi memainkan peran yang lebih signifikan. Contoh kasus : Penggunaan komputer untuk pedophilia melalui internet.

Modus Operandi *Cybercrime*

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada antara lain (Golose, 2006) :

a. Unauthorized Access to Computer System and Service

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer sec
atau tan sepengetah

jaringan komputer yang dimasukinya. 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).

b. 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, 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

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. Misalnya kasus www.Klikbca.com oleh *hacker* Steven Haryanto

d. Cyber Espionage

Kejahatan yang memanfaatkan jaringan Internet untuk melakukan kegiatan matamata 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)

e. Cyber Sabotage and Extortion

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. Misalnya dengan penyebaran Virus komputer saat korban melakukan browsing di internet.

f. 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.

g. Infringements of Privacy

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.

Pencegahan dan Penanggulangan *Cybercrime*

Tindak pidana *cybercrime* memakan korban yang tidak sedikit jumlahnya, terutama dari sisi finansial. Sebagian besar korban hanya bisa menyesali apa yang sudah terjadi. Mereka berharap bisa belajar banyak dari pengalaman yang ada, yang perlu dilakukan sekarang adalah melakukan pencegahan terhadap kemungkinan-kemungkinan yang dapat merugikan kita sebagai pelaku IT. Pencegahan itu dapat berupa:

- *Educate User* (memberikan pengetahuan baru terhadap *Cyber Crime* dan dunia internet)
- *Use hacker's perspective* (menggunakan pemikiran dari sisi *hacker* untuk melindungi sistem Anda)
- *Patch System* (menutup lubang-lubang kelemahan pada sistem)
- *Policy* (menentukan kebijakan-kebijakan dan aturan-aturan yang melindungi sistem Anda dari orang-orang yang tidak berwenang)

  IDS *(Intrusion Detection System) bundled with IPS (Intrusion Prevention System)*
- *Firewall*
- AntiVirus

Beberapa langkah penting yang harus dilakukan dalam penanggulangan *Cybercrime* adalah :

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
b. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *Cybercrime*
d. Meningkatkan kesadaran warga negara mengenai masalah *Cybercrime* serta pentingnya mencegah kejahatan tersebut terjadi
e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *Cybercrime*, antara lain melalui perjanjian ekstradisi dan mutual *assistance treaties.*

Contoh bentuk penanggulangan yang lain :

1. *IDCERT (Indonesia Computer Emergency Response Team)*

   Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya *"sendmail worm"* (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah Computer EmergencyResponse Team (CERT) Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi *point of contact* bagi orang untuk melaporkan masalah kemanan. IDCERT merupakan CERT Indonesia.

2. Sertifikasi perangkat *security*

   Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia.

Tindakan Hukum bagi pelaku *Cybercrime*

Cybercrime law dan regulasi yang tepat di bidang ICT dianggap penting dalam menarik investasi maupun pengembangan perekonomian yang berbasis IT. *Cybercrime* potensial menimbulkan kerugian pada beberapa bidang : politik, ekonomi, sosial budaya yang lebih besar dampaknya dibandingkan dengan kejahatan yang berintensitas tinggi lainnya. Di masa mendatang dapat menganggu perekonomian nasional melalui jaringan infrastruktur yang berbasis teknologi elektronik (perbankan, telekomunikasi satelit, jaringan listrik, dan jaringan lalu lintas penerbangan Ishak, 2002 (dalam Setiyadi, 2003).

Menjawab tuntutan dan tantangan komunikasi global lewat Internet, Undang-Undang yang diharapkan (*ius konstituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan Internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi. Peraturan dan perundangan di bidang ICT termasuk *Cybercrime law* diperlukan karena (setiyadi, 2003):

1. Melindungi integritas pemerintah dan menjaga reputasi suatu negara.

2. Membantu negara terhindar dari menjadi surga bagi pelaku kejahatan, seperti teroris, kejahatan terorganisasir, dan operasi penipuan.
3. Membantu negara terhindar dari sebutan sebagai tempat yang nyaman untuk menyimpan aplikasi atau data hasil kejahatan cybercrime.
4. Meningkatkan kepercayaan pasar karena adanya kepastian hukum yang mampu melindungi kepentingan dalam berusaha.
5. Memberikan perlindungan terhadap data yang tergolong khusus (*classified*), rahasia, informasi yang bersifat pribadi, data pengadilan kriminal, dan data publik yang dianggap perlu untuk dilindungi.
6. Melindungi konsumen, membantu penegakan hukum, dan aktivitas intelligen. Mencegah korupsi.
7. Meningkatkan keamanan nasional dan mengurangi kerentanan dari serangan dan aksi oleh teroris dan mereka yang berniat jahat.
8. Melindungi dunia usaha dari resiko bisnis seperti kehilangan pangsa pasar, rusaknya reputasi, penipuan, tuntutan hukum dari publik, dan kasus perdata maupun pidana.
9. Sebagai sarana untuk menghukum pelaku kejahatan di bidang teknologi informasi.
10. Meningkatkan peluang bagi diakuinya catatan elektronik sebagai alat bukti yang sah di pengadilan dalam kasus kejahatan biasa seperti pencurian, penipuan, pembunuhan, penculikan dan lain – lain, atau kejahatan komputer dan kejahatan yang dilakukan menggunakan Internet.

Pengaturan hukum dalam Internet masih relatif baru dan terus berkembang, ada dorongan pengaturan yang bersifat global, namun kedaulatan hukum menjadikannya tidak mudah terlaksana. Hal ini menjadi salah satu kelemahan dari penegakan *cybercrime law* terutama jika menyangkut perkara kejahatan yang dilakukan oleh individu atau entitas bisnis yang berada di negara lain. Konstitusi suatu negara tidak dapat dipaksakan kepada negara lain karena dapat bertentangan dengan kedaulatan dan konstitusi negara lain, oleh karena itu hanya berlaku di negara yang bersangkutan saja, seperti pada kasus berikut :

- Yahoo vs Perancis: Yahoo menjual atribut Nazi yang dilarang di Perancis
- Google vs China: Pemerintah China memblokir situs Google dan mengalihkan ke situs pemerintah.

Kasus *Cybercrime* terjadi hampir di setiap negara di dunia dan masing-masing negara mempunyai cara penanganan yang berbeda, (Rahardjo, 2001):

1. Amerika Serikat memiliki:
   a) Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Departement of Justice. Institusi ini memiliki situs web <http://www.cybercrime.gov> yang memberikan informasi tentang cybercrime. Namun banyak informasi yang masih terfokus kepada computer crime.
   b) b. *National Infrastructure Protection Center* (NIPC) merupakan sebuah institusi pemerintah Amerika Serikat yang menangani masalah yang berhubungan dengan infrastruktur. Institusi ini mengidentifikasi bagian infrastruktur yang penting (*critical*) bagi negara (khususnya bagi Amerika Serikat). Situs web: <http://www.nipc.gov>. Internet atau jaringan komputer sudah dianggap sebagai infrastruktur yang perlu mendapat perhatian khusus. Institusi ini memberikan *advisory*
2. The National Information Infrastructure Protection Act of 1996
3. CERT yang memberikan *advisory* tentang adanya lubang keamanan *(Security holes).*
4. Korea memiliki *Korea Information Security Agency* yang bertugas untuk melakukan evaluasi perangkat keamanan komputer & Internet, khususnya yang akan digunakan oleh pemerintah.

Saat ini, Indonesia belum memiliki Undang - Undang khusus/ *cyber law* yang mengatur mengenai *cybercrime* walaupun rancangan undang undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari ra[illegible] undang undang tindak pidana di bidang [illegible] tahun 200[illegible]h dikirim[illegible]

RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki. Dalam Upaya Menangani kasus-kasus yg terjadi khususnya yang ada kaitannya dengan *Cybercrime*, para Penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP Pasal yang dapat dikenakan dalam KUHP pada *Cybercrime* antara lain:

1. KUHP (Kitab Undang-Undang Hukum Pidana), pasal-pasal yang terkait :

a. Pasal 362 KUHP tentang pencurian (Kasus carding) Carding sendiri dalam versi POLRI meliputi (Arifiyadi, 2008):
   i. Mendapatkan nomor kartu kredit (CC) dari tamu hotel, khususnya orang asing
   ii. Mendapatkan nomor kartu kredit melalui kegiatan chatting di Internet
   iii. Melakukan pemesanan barang ke perusahaan di luar negeri dengan menggunakan Jasa Internet
   iv. Mengambil dan memanipulasi data di Internet.
   v. Memberikan keterangan palsu, baik pada waktu pemesanan maupun pada saat pengambilan barang di Jasa Pengiriman (kantor pos, UPS, Fedex, DHL, TNT, dan lain-lain.). *Carding* (pelakunya biasa disebut *carder*), adalah kegiatan melakukan transaksi e-commerce dengan nomor kartu kredit palsu atau curian. Pelaku tidak harus melakukan pencurian atau pemalsuan kartu kredit secara fisik, melainkan pelaku cukup mengetahui nomor kartu dan tanggal kadaluarsanya saja .
b. Pasal 378 KUHP tentang Penipuan (Penipuan melalui website seolah-olah menjual barang)
c. Pasal 311 KUHP Pencemaran nama Baik (melalui media internet dengan mengirim email kepada Korban maupun teman-teman korban)
d. Pasal 303 KUHP Perjudian (permainan judi online)
e. Pasal 282 KUHP Pornografi (Penyebaran pornografi melalui media internet).
f. Pasal 282 dan 311 KUHP (tentang kasus Penyebaran foto atau film pribadi seseorang yang vulgar di Internet).
g. Pasal 378 dan 362 (tentang kasus Carding karena pelaku melakukan penipuan seolah-olah ingin membayar, dengan kartu kredit hasil curian)

2. Undang-Undang No.19 Thn 2002 tentang Hak Cipta, Khususnya tentang Program Komputer atau software
3. Undang-Undang No.36 Thn 1999 tentang Telekomukasi, (penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi).
4. Undang-undang No.25 Thn 2003 tentang Perubahan atas Undang-Undang No.15 Thn 2002 tentang Pencucian Uang.
5. Undang-Undang No.15 thn 2003 tentang Pemberantasan Tindak Pidana Terorisme.

Hambatan dalam penanganan *Cybercrime*

Meskipun sudah ada beberapa pasal yang bisa menjerat pelaku *Cybercime* ke penjara masih dijumpai adanya hambatan-hambatan dalam pelaksanaan di lapangan yang antara lain sebagai berikut (Noor, 2005):

1) Perangkat hukum yang belum memadai

Para penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP sependapat bahwa perlu dibuat undang-undang yang khusus mengatur *cybercrime*.

2) Kemampuan penyidik

Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap *hacking* komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (determinan) adalah:

a. Kurangnya pengetahuan tentang komputer.
b. Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus *Cybercrime* masih terbatas.
c. Faktor sistem pembuktian yang menyulitkan para penyidik.

3) Alat Bukti

Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap *Cybercrime* antara lain berkaitan dengan karakteristik kejahatan *cybercrime* itu sendiri, yaitu ; sasaran atau media *cybercrime* adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya, *Cybercrime* seringkali dilakukan hampir-hampir tanpa saksi, di sisi lain, saksi korban seringkali berada jauh di luar negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan..

4) Fasilitas komputer forensik

Untuk membuktikan jejak-jejak para *hacker*, dan *cracker* dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa *soft copy* (image, program, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas *forensic computing* yang memadai. Fasilitas *forensic computing* yang akan didirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu *evidence collection, forensic analysis*, *expert witness*.

SIMPULAN

Dari pembahasan diatas dapat diperoleh beberapa kesimpulan :

1) Opini umum yang terbentuk bagi para pemakai jasa internet adalah bahwa *Cybercrime* merupakan perbuatan yang merugikan. Para korban menganggap atau memberi stigma bahwa pelaku *Cybercrime* adalah penjahat. Modus operandi *Cybercrime* sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi, tetapi jika diperhatikan lebih seksama akan terlihat bahwa banyak di antara kegiatan-kegiatan tersebut memiliki sifat yang sama dengan kejahatan-kejahatan konvensional. Perbedaan utamanya adalah bahwa *Cybercrime* melibatkan komputer dalam pelaksanaannya. Kejahatan-kejahatan yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer perlu mendapat perhatian khusus, sebab kejahatan-kejahatan ini memiliki karakter yang berbeda dari kejahatan-kejahatan konvensional.

2) Sistem perundang-undangan di Indonesia belum mengatur secara khusus mengenai kejahatan komputer melalui media internet. Beberapa peraturan yang ada baik yang terdapat di dalam KUHP maupun di luar KUHP untuk sementara dapat diterapkan terhadap beberapa kejahatan, tetapi ada juga kejahatan yang tidak dapat diantisipasi oleh undang-undang yang saat ini berlaku.

3) Hambatan-hambatan yang ditemukan dalam upaya melakukan penyidikan terhadap *Cybercrime* antara lain berkaitan dengan masalah perangkat hukum, kemampuan penyidik, alat bukti, dan fasilitas komputer forensik. Upaya-upaya yang dapat dilakukan untuk mengatasi hambatan yang ditemukan di dalam melakukan penyidikan terhadap *Cybercrime* antara lain berupa penyempurnaan perangkat hukum, mendidik para penyidik, membangun fasilitas *forensic computing*, meningkatkan upaya penyidikan dan kerja sama internasional, serta melakukan upaya penanggulangan pencegahan.

SARAN

Beberapa hal yang dapat dijadikan sebagai saran sehubungan dengan hasil penelitian terhadap *Cybercrime* adalah sebagai berikut :

1) Undang-undang tentang *Cybercrime* perlu dibuat secara khusus sebagai *lexspesialis* untuk memudahkan penegakan hukum terhadap kejahatan tersebut.

2) Kualifikasi perbuatan yang berkaitan dengan *Cybercrime* harus dibuat secara jelas agar tercipta kepastian hukum bagi masyarakat khususnya pengguna jasa internet.

3) Perlu hukum acara khusus yang dapat mengatur seperti misalnya berkaitan dengan jenis-jenis alat bukti yang sah dalam kasus *Cybercrime*, pemberian wewenang khusus kepada penyidik dalam melakukan beberapa tindakan yang diperlukan dalam rangka penyidikan kasus *Cybercrime*, dan lain-lain.

4) Spesialisasi terhadap penuntut umum dan

salah satu cara untuk melaksanakan penegakan hukum terhadap *Cybercrime*.

DAFTAR PUSTAKA

Arifiyadi Teguh, (2008), ” Menjerat Pelaku Cyber Crime dengan KUHP”, Pusat Data Departemen Komunikasi dan Informatika diakses pada tanggal 3 Maret 2009 dari www. depkominfo.go.id

----------, (2008), ”*Cybercrime* dalam Perspektif Rancangan Konsep KUHP Baru”, Pusat Data Departemen Komunikasi dan Informatika diakses pada tanggal 3 Maret 2009 dari www. depkominfo.go.id

Fajri, Anthony, April 2008, ”Cybercrime” http://students.ee.itb.ac.id/fajri/publication

Golose, PetrusReinhard, 2006, ”Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia oleh Polri”, Buletin Hukum Perbankan dan Kebanksentralan Vol.4 Nomor.2 Agustus 2006

Gregory, Thomas HA, 2005 ”Ketenaran Cybercrime di Indonesia”, Makalah STIMIK Perbanas 2005 yang dipublikasikan diakses pada 19 Desember 2008 di www.google.com

Noor, Azamul Fadhly, 2005, ”Tinjauan Yuridis terhadap Cybercrime di Indonesia”, Tesis pada Program Studi Magister Ilmu Hukum Program Pascasarjana Universitas Sumatra Utara, yang dipublikasikan

Mc Leod Jr, Rayman and Schell, George P, April 2008, “ Sistem Informasi Manajemen” Edisi 10, Penerbit Salemba Empat

Rahardjo, Budi, 2001, ”Cybercrime”, draft pada diskusi mengenai topik yang sama br@paume.itb.ac.id – budi@cert.or.id

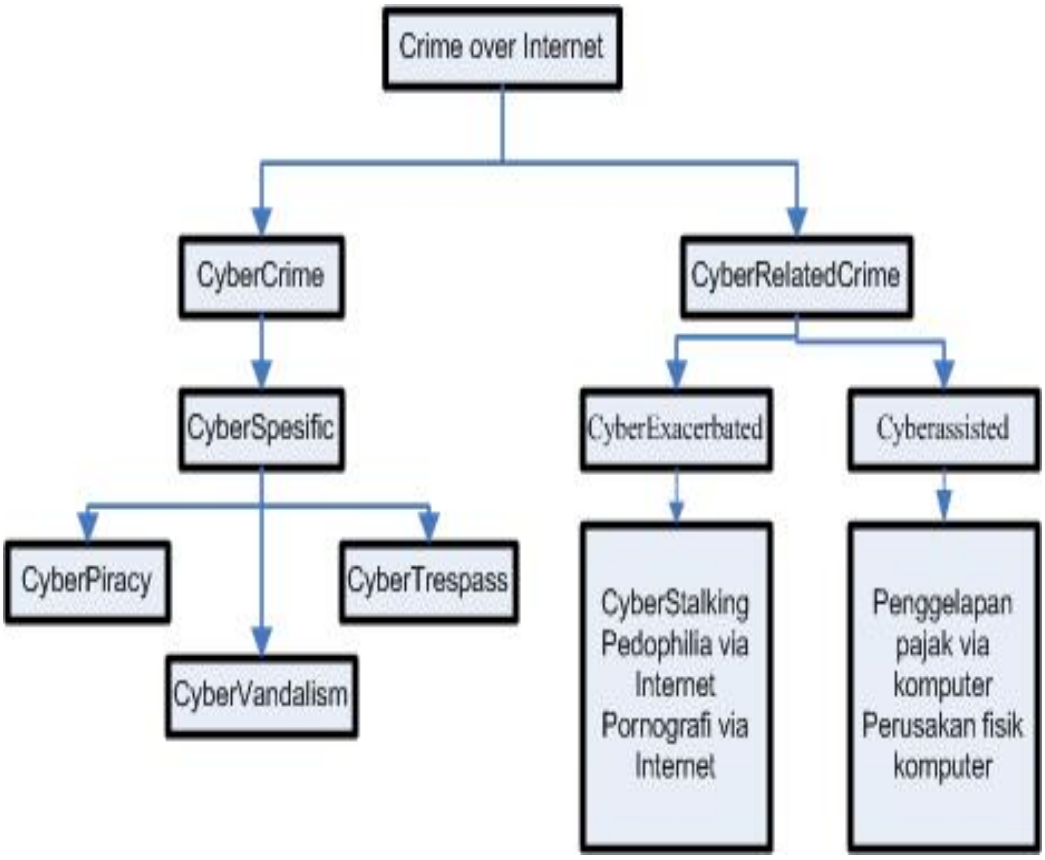
Setiyadi, Mas Wigrantoro Roes, 2003, “Urgensi Cybercrime Law sebagai Perlindungan bagi Pengguna Teknologi Informasi” Pendekatan Kebijakan Publik Dalam Menjawab Kebutuhan Terhadap Perangkat Legal Untuk Memerangi Kejahatan Di Bidang Teknologi Informasi (Cybercrime), Makalah disampaikan pada Cybercrime Seminar 19 Maret 2003

Sinar Indonesia Baru, 2009, “Kasus “Cyber Crime” Indonesia Tertinggi di Dunia”, diakses pada 29 Maret 2009 di www.google.com

Tahir, Achmad, April 2009, “Penegakan Hukum Cybercrime di Indonesia”, Tesis pada Program Studi Magister Ilmu Hukum Program Pascasarjana Universitas Gajah Mada, yang dipublikasikan

LAMPIRAN

Jenis dan Penggolongan Cybercrime



Sumber : Fajri, 2008