Terakreditasi Dirjen Dikti SK No. 56/DIKTI/Kep/2005

"Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia

M.E. Fuady

ABSTRACT

It had been long known that technology, as Janus, has two side of coins: the good side, and the bad side. Everybody knows the benefit of technology development. But there aren't much who realize the negative potent of technology. Cybercrime discussed in this article is an example of how crime was developed sophisticatedly by using technological means. Cybercrime, simply defined as criminal acts using cyber and Internet, has faced a new challenge for lawmaker and law enforcement mission. In Indonesia, carding become serious issues to be combated. Another type of cybercrime frequently occur in Indonesia are hacking and deface. Although Internet user in Indonesia is estimated no more than 5% of total population (4.38 million persons), everybody must attended cybercrime issues seriously. The loss of cybercrime reached unspeakable heights and damaged public safety in communication and information flows.

Kata kunci: "cybercrime", realitas virtual, dunia tanpa batas

Internet: Teknologi Pencipta Dunia "Cyber"

Kehadiran teknologi komunikasi modern seperti internet telah membuat pandangan manusia mengenai kehidupan berubah. Paradigma komunikasi manusia dalam menjalani aktivitas ekonomi, bisnis, interaksi sosial, dan politik, menjadi berbeda. Sebelumnya, manusia didominasi oleh aktivitas yang bersifat fisik, *face to face*. Manusia dihalangi oleh berbagai keterbatasan. Dengan internet, ruang, jarak, dan waktu yang membatasi manusia menghilang. Menurut Kenichi Ohmae (Mahayana, 1999:97), itulah dunia tanpa batas (*the borderless world*).

Internet merupakan jaringan dari jutaan komputer yang saling terhubungkan. Dengan internet, setiap orang di seluruh dunia dapat berkomunikasi hanya dengan menekan *keyboard* dan *mouse* di hadapannya. Informasi apa pun yang dibutuhkan telah tersedia. Karena kemudahan yang ditawarkan itulah banyak individu yang menggunakannya. Dibandingkan radio dan televisi, penetrasi internet di kalangan masyarakat, termasuk yang paling cepat. Untuk mencapai pengguna sebanyak 50 juta orang, internet hanya membutuhkan waktu 5 tahun, sementara radio membutuhkan waktu 38 tahun dan televisi 13 tahun (Temporal & Lee, 2002:7). Saat ini, diperkirakan pengguna internet telah mencapai 220 juta orang.

Dengan menggunakan internet, *user* berkesempatan untuk berpetualang, berkelana, berselancar menelusuri *cyberspace*, sebuah dunia komunikasi berbasis komputer (*computer mediated communication*). Realitas yang ditawarkan adalah realitas virtual, kehadirannya tidak dapat ditangkap

atau dipegang tangan, tetapi dikonstruksikan secara sosial oleh orang-orang yang menggeluti teknologi komunikasi dan informasi. Realitas *cyberspace* adalah kenyataan yang melampaui dan artifisial (*hyperreal*). Menurut Piliang (2001), karena rekayasa sedemikian rupa, kenyataan (*real*) ditutupi oleh tanda kenyataan (*sign of real*) sedemikian rupa, sehingga antara tanda dan relitas, antara model dan kenyataan, tidak lagi dapat dibedakan.

Cyberspace menawarkan segala hal yang diperlukan manusia, termasuk kesenangan, keuntungan, dan kemudahan tanpa bersusah payah menggerakkan badan untuk memeroleh sesuatu. Berbagai informasi gratis dari surat kabar dalam dan luar negeri dapat diperoleh tanpa membeli. Menikmati musik tanpa harus membeli kaset. Bagi dosen, berbagai literatur tersaji secara gratis tanpa harus pergi ke tempat berada. Inilah "zona mabuk teknologi" yang dikemukakan Philips dan Naisbitt (2001).

Kehidupan virtual yang disajikan *cyberspace* telah memunculkan bentuk aktivitas baru untuk mencapai kepuasan, seperti *teleshopping*, *teleconference*, *virtual gallery*, *virtual museum*, *e-commerce*, namun juga memunculkan penyimpangan-penyimpangan seperti kejahatan dengan memanfaatkan internet atau *cybercrime*.

"Cybercrime": Bentuk Kejahatan di Dunia Maya

Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime. The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai:"…*any illegal act requiring knowledge of 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*". Hamzah (1989) mengartikan: "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dari beberapa pengertian di atas, Wisnubroto (1999) merumuskan *computer crime* sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas, *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih. Selanjutnya, disebabkan kejahatan itu dilakukan di ruang *cyber* melalui internet, muncul istilah *cybercrime*.

Bagi sebagian besar masyarakat yang terbiasa menggunakan media teknologi komunikasi (telekomunikasi), *cybercrime* bukanlah istilah yang asing terdengar. *Cybercrime* atau kejahatan di ruang maya merupakan sebuah fenomena yang tidak terbantahkan. Tidak terlihat namun nyata. Terdapat berbagai kasus *cybercrime* yang kian hari kian meningkat, terutama di negara-negara yang tidak memiliki kepastian hukum dalam bidang teknologi komunikasi modern (*convergence*).

Teknologi komunikasi yang memiliki kekuatan dahsyat dalam merubah perilaku komunikasi manusia, selain membawa keuntungan berupa kemudahan dalam berkomunikasi, ternyata memiliki "sisi gelap". Teknologi membawa kerugian, salah satunya berupa semakin dipermudahkannya "penjahat" dalam melakukan kejahatannya. Kecanggihan teknologi memungkinkan penjahat *cyber* memangsa korban-korbannya. Meski tidak mau disebut sebagai pelaku kriminal, sebagai akibat dari perbuatannya, mereka tidak ada bedanya dengan seorang penjahat.

Menurut Raharjo (2002:29), sebagai sebuah gejala sosial, kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern). Kejahatan konvensional di dunia nyata muncul dalam dunia maya (*virtual*) dengan wajah kejahatan yang telah diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau *cybercrime* membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, tidak merasakannya sebagai sebuah bentuk kejahatan. Padahal, sudah begitu banyak korban (*victim*) dan

kerugian moril dan materil akibat *cybercrime*. Korbannya dapat berupa *netizen* (penduduk dunia *virtual*/penghuni *cyberspace*) dan masyarakat luas yang awam.

Perusahaan yang bergerak dalam bidang bisnis dan individu tak berdosa, yang tidak memiliki keahlian bahkan pemahaman akan teknologi komunikasi, dapat menjadi korban. Tidak perlu jauh-jauh, kita semua masih ingat dengan kasus mahasiswa dan artis "bugil" yang beredar di internet. Sedikit sekali di antara mereka yang memahami teknologi komunikasi, tetapi mereka telah menjadi korban. Sebut saja artis dengan inisial YS, KD, KF, CK, dan masih banyak lagi. Itu salah satu contoh kecil korban dari *cybercrime*. Meski memang ada publik yang tidak menyepakati *cyberporn* sebagai *cybercrime*. Tetapi, kita telah melihat adanya korban akibat perbuatan pelaku *cybercrime*. Sebagai catatan penting, menurut Menteri Negara Komunikasi dan Informasi, sekitar 50 persen kalangan muda yang menggunakan internet lebih suka untuk mengunjungi situs porno (*Kompas Cyber Media*, 05 Mei 2002).

Untuk memahami *cybercrime*, perlu kiranya dipahami terlebih dahulu apa yang disebut dengan *hacker*, *cracker* dan beberapa lainnya. Karena, seperti halnya kehidupan nyata, ada di antara mereka yang "hitam" dan "putih", ada yang berlaku seperti pahlawan dan penjahat.

(1) *Hacker*

Hacker secara harfiah berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup melalui komputer ke dalam jaringan komputer (*Republika*, 22 Agustus 1999). Menurut Ustadiyanto (2001:304), ada definisi yang relevan, yakni *hacker* adalah orang-orang yang ahli dalam bidangnya. Bila komputer, maka dia pandai menggunakannya. Ia sangat menguasai komputer. *Hacker* adalah orang-orang yang gemar mempelajari seluk-beluk sistem komputer dan bereksperimen dengannya. Mereka pandai untuk menyusup ke dalam jaringan komunikasi suatu institusi di dunia maya. *Hacker* menjunjung tinggi etika atau norma yang berlaku di dunia maya. Mereka anti penyensoran, anti penipuan, dan pemaksaan kehendak pada orang lain. Mereka memegang prinsip bahwa meng-*hack* untuk tujuan meningkatkan keamanan jaringan internet. Misalnya, bila ada sebuah perusahaan perbankan mengatakan bahwa jaringan sistem komunikasi mereka sudah sangat canggih dan mustahil dibobol, tidak dapat ditembus oleh siapa pun, maka *hacker* tertantang untuk mencoba dan setelah berhasil mereka memperingatkan betapa lemahnya sistem informasi perusahaan terrsebut. Oleh karena itu, tidak sedikit dari mereka yang akhirnya direkrut perusahaan untuk mengamankan sistem informasi dan komunikasi di dunia maya.

(2) *Cracker*

Di dunia *cyber*, ada pula *hacker* yang memiki sisi gelap. Mereka disebut *cracker*. Para *cracker* ini secara ilegal melakukan penyusupan dan perusakan terhadap situs, *website,* dan sistem keamanan jaringan internet untuk memperoleh kesenangan dan keuntungan. Mereka bangga dan sombong atas keberhasilan mereka merusak situs sebuah perusahaan. Serangannya sangat luar biasa. Kementerian Petahanan Amerika Serikat di Pentagon mencatat serangan 100 *cracker* dalam satu hari (*Republika*, 6 Januari 2000).

(3) *Carder*

Carder adalah orang yang melakukan *cracking*, yakni pembobolan terhadap kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk kepentingan pribadi. Biasanya yang menjadi korbannya adalah mereka yang memiliki kartu kredit dalam jumlah besar. Menurut hasil riset, pada tahun 2002, Indonesia menempati urutan kedua setelah Ukraina dalam kejahatan *carding*.

(4) *Deface*

Deface adalah tindakan menyusup ke suatu situs, lalu mengubah tampilan halaman dari situs dengan tujuan tertentu. Indonesia pernah diserang para *deface* yang mengubah situs TNI. Tampilan gambar Burung Garuda Pancasila diganti dengan lambang palu arit. *Hompage* Polri diganti tampilannya dengan

gambar wanita telanjang.

(5) *Phreaker*
*Yaitu ses*eorang yang melakukan *cracking* terhadap jaringan telepon, sehingga dapat menelepon secara gratis ke daerah manapun yang dituju (*Komputeraktif*, No. 43/18 Desember 2002). Di Indonesia, kasus semacam ini pernah terjadi pada wartel–wartel.

Para pelaku *hacking* biasanya bukan dari kalangan lapisan bawah, pada umumnya mereka adalah kaum terpelajar, setidak-tidaknya mengenyam pendidikan formal sampai tingkat tertentu dan dapat menggunakan atau mengoperasikan komputer. Para *craker* adalah orang yang berpendidikan, tidak buta teknologi, secara ekonomis mampu dan tidak termasuk dalam masyarakat lapisan bawah. Kejahatan ini dapat dikategorikan kepada *white collar crime* (kejahatan kerah putih). Jo Ann L. Miller, mengkategorikan pelakunya menjadi 4 (empat).

(a) *Organizational occupational crime*
Pelakunya adalah para eksekutif. Mereka melakukan perbuatan ilegal atau merugikan orang lain melalui jaringan internet demi kepentingan atau keuntungan korporasi.

(b) *Government occupational crime*
Pelakunya adalah pejabat atau birokrat yang melakukan perbuatan ilegal melalui internet atas persetujuan atau perintah negara atau pemerintah, meski dalam banyak kasus, bila terungkap hal itu akan disangkal.

(c) *Professional occupational crime*
Berbagai profesi yang melakukan kejahatan secara sengaja (*malpractice*).

(d) *Individual occupational crime*
Perilaku menyimpang yang dilakukan oleh para pengusaha, pemilik modal atau orang-orang independen lainnya, walau mungkin tidak tinggi tingkat sosial ekonominya. Dalam bidang kerjanya kalangan ini memilih jalan yang menyimpang yang melanggar hukum atau merugikan orang lain.

Karakteristik "Cybercrime"

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain (CYBERCRIME_files\ inline_files\ SI10.HTM):

(1) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/ wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.

(2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.

(3) Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional

(4) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya

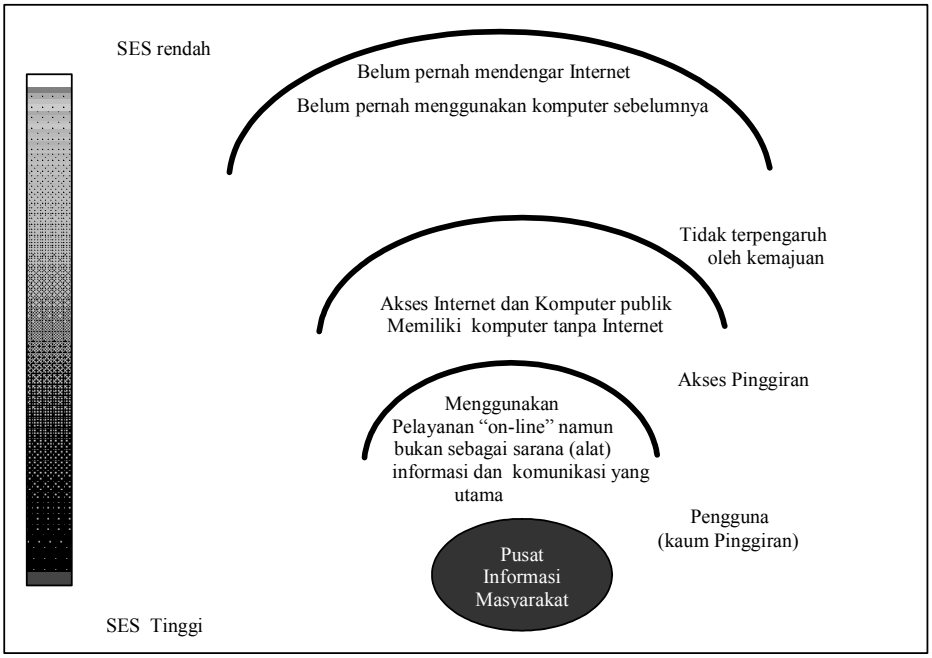
(5) Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

"Cybercrime" di Indonesia

Di antara negara berkembang, Indonesia termasuk negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia tidak memrioritaskan strategi pengembangan dan penguasaan teknologi. Yang terjadi kemudian, transfer teknologi dari negara maju tidak serta merta diikuti dengan penguasaan teknologi oleh negara berkembang seperti Indonesia. Bandingkan saja dengan Malaysia yang telah memproduksi secara massal *software*, per*sonal Computer* (PC), dan ponsel. Sungguh ironis memang, karena menjelang 1980-an Indonesia adalah negara Asia Tenggara pertama yang memiliki satelit komunikasi. Singapura dan Malaysia yang saat itu masih menyewa satelit Palapa dari Indonesia, kini menjadi negara maju berbasis teknologi komunikasi modern.

Meski masih diperdebatkan, dapat dikatakan Indonesia merupakan negara yang memiliki kesenjangan digital yang cukup lebar. Kesenjangan digital dapat diartikan sebagai adanya jurang di antara mereka yang mampu mengakses teknologi komunikasi dan yang tidak mampu (Staubhaar & La Rose, 2000:9). Selain masih senjangnya tingkat pendidikan dan ekonomi di Indonesia, kesempatan

Gambar 1: Model Pusat-Pinggiran Akses Teleteknologi



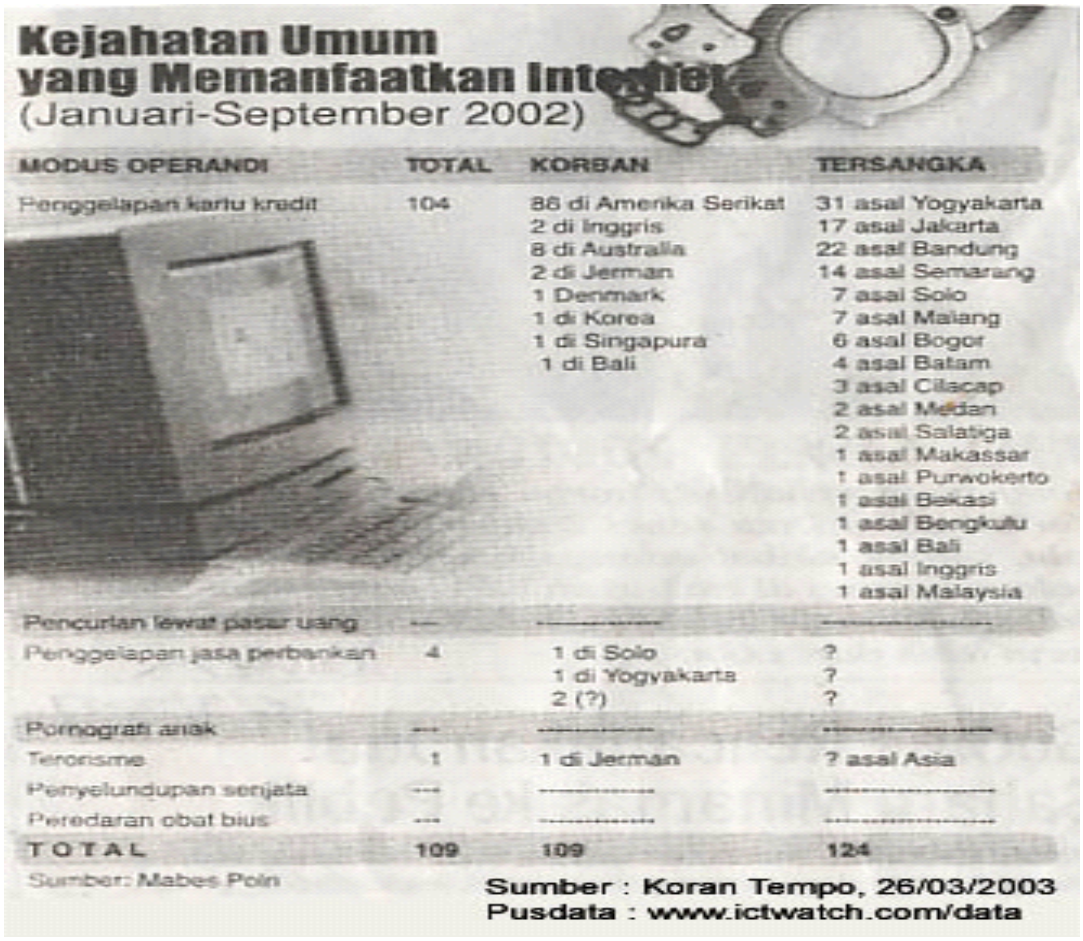
Sumber: Wilhelm (2003:119)

untuk menggunakan teknologi komunikasi di Indonesia belum merata. Ketimpangan, ketidakmilikan informasi dan telekomunikasi dapat dibagi dalam beberapa kategori. Yang paling banyak aksesnya, tentu saja, yang paling dekat dengan pusat informasi masyarakat.

Meskipun terdapat kesenjangan digital, di Indonesia marak sekali kejahatan *cyber*. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para *hacker* hitam. Mereka bisa memperoleh barang apa pun yang diinginkan, mulai dari berlian, radar laut, *corporate software*, *computer server*, Harley Davidson, hingga senjata M-16 (*Warta Ekonomi.com*, 23 Desember 2002) dengan menggunakan kartu kredit milik orang lain. Istilahnya adalah c*arding*. Para *carder* (*hacker* hitam) memesan barang-barang melalui internet untuk dikirimkan ke negara mereka berada. Barang yang dipesan dapat digunakan sendiri, dapat pula dijual dengan harga yang sangat murah. Misalnya, *Notebook* bermerk *Sony* seharga 20 Juta yang dipesan melalui *carding*, dijual seharga 4 Juta rupiah. Untuk yang satu ini, *ClearCommerce*, perusahaan keamanan internet yang berbasis di Texas, Amerika Serikat, memasukkan Indonesia ke dalam daftar negara-negara terburuk untuk kejahatan yang memanfaatkan kecanggihan teknologi komunikasi. Setidaknya, 20 persen transaksi kartu kredit internet yang berasal dari Indonesia merupakan penipuan. Berikut ini adalah data kejahatan yang memanfaatkan internet:

Dari data di bawah (*Koran Tempo*, 26 Maret 2003), Yogyakarta menempati urutan pertama dan Bandung kedua dalam *cybercrime* jenis *carding di* Indonesia. Yang melakukan jenis kejahatan itu adalah kalangan muda, biasanya mahasiswa. Seorang mahasiswa universitas swasta di Bandung pernah memesan 5 buah ponsel *Nokia Communicator* yang ia jual seharga 5 Juta rupiah, padahal saat itu harganya berkisar 10 Juta rupiah.

Gambar 2: Kejahatan Umum yang Memanfaatkan Internet



Kejahatan Umum yang Memanfaatkan Internet
(Januari-September 2002)

MODUS OPERANDI	TOTAL	KORBAN	TERSANGKA
Penggelapan kartu kredit	104	86 di Amerika Serikat 2 di Inggris 8 di Australia 2 di Jerman 1 Denmark 1 di Korea 1 di Singapura 1 di Bali	31 asal Yogyakarta 17 asal Jakarta 22 asal Bandung 14 asal Semarang 7 asal Solo 7 asal Malang 6 asal Bogor 4 asal Batam 3 asal Cilacap 2 asal Medan 2 asal Salatiga 1 asal Makassar 1 asal Purwokerto 1 asal Bekasi 1 asal Bengkulu 1 asal Bali 1 asal Inggris 1 asal Malaysia
Pencurian lewat pasar uang	---	----------	----------
Penggelapan jasa perbankan	4	1 di Solo 1 di Yogyakarta 2 (?)	? ? ?
Pornografi anak	---	----------	----------
Terorisme	1	1 di Jerman	? asal Asia
Penyelundupan senjata	---	----------	----------
Peredaran obat bius	---	----------	----------
TOTAL	109	109	124

Sumber: Mabes Polri

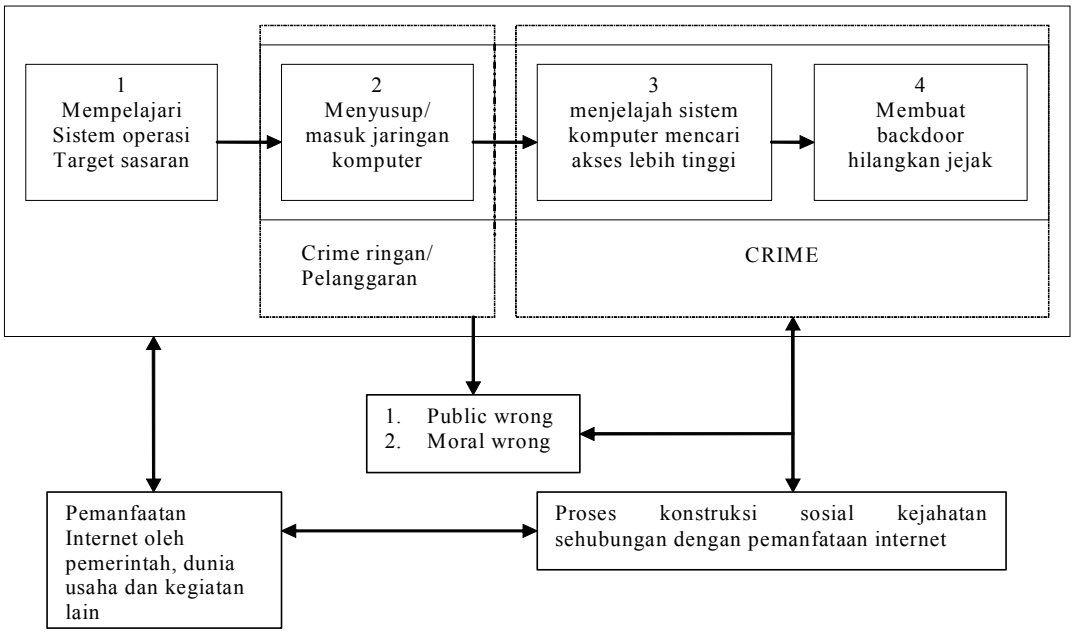
Sumber : Koran Tempo, 26/03/2003
Pusdata : www.ictwatch.com/data

Agar tidak diketahui identitasnya, ia melakukan *carding* di warnet sekitar kampus dan saat mengambil pesanan, agar dimudahkan, ia bekerjasama dan memberi sejumlah uang kepada oknum karyawan biro pengiriman paket terkemuka di Indonesia.

Indonesia tampaknya akan semakin mengukuhkan diri sebagai negara kampiun penipuan kartu kredit di internet Dalam berbagai urusan yang berkonotasi buruk, Indonesia memang seringkali termasuk di dalamnya, mulai dari pendapatan perkapita yang rendah, mutu pendidikan, tingkat korupsi, termasuk *cybercrime* jenis *carding*.

Kejahatan memang tidak dapat diprediksi kejadiannya, tidak mempedulikan tempat dan suasana ketika hendak muncul, tidak pula membanding-bandingkan siapa pelaku dan korbannya, tidak mengenal kasta ataupun status sosial pelaku dan korbannya. Saat muncul, ia dapat menjadi bahan yang menarik untuk dibicarakan, baik di media massa maupun ruang-ruang seminar. Apalagi saat kejahatan itu dipadukan dengan kecanggihan teknologi komunikasi. Tanpa sadar

Gambar 3. Bagan Konstruksi Kejahatan dari "Hacking"



Sumber: Raharjo (2002)

di sekeliling kita terdapat kejahatan yang "*innocent*", seolah tanpa dosa dan begitu halus.

Adapun konstruksi kejahatan *Hacking* dapat dilihat pada gambar 3.

Selain *cybercrime* jenis *carding*, di Indonesia juga sering terjadi kasus *deface*. Tampilan situs di Internet dirusak dan diganti oleh para *hacker* hitam. Berikut ini adalah kasus-kasus yang pernah terjadi (Raharjo, 202:35):

(a) Tahun 1997 ketika masalah Timor-Timur menghangat, situs milik Departemen Luar Negri dan ABRI (TNI, pen) dijebol oleh *craker Porto* (Portugis) yang pro-kemerdekaan. Mereka juga merusak situs-situs bisnis dan pendidikan. Serangan dari *craker* Porto ini mendapat balasan dari *craker* Indonesia. Hal ini dilakukan karena, menurut mereka, *craker* Porto dinilai keterlaluan, serangannya membabi-buta, tidak mempedulikan apakah itu situs milik pemerintah ataupun bukan, situs bisnis maupun situs pendidikan.
(b) Tahun 1998, tampilan depan atau *frontpage* Pusat Dokumentasi Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) diganti dengan gambar wanita telanjang.
(c) Tahun 1998, setelah kerusuhan 13–14 Mei, *craker* yang diduga berasal dari Cina menghantam situs milik pemerintah, yaitu BKKBN. Serangan ini merupakan reaksi atas pemberitaan media mengenai kerusuhan Mei yang menyebabkan etnis Cina di Indonesia menjadi korban pembantaian dan pemerkosaan.
(d) Juni 1999, *homepage* POLRI diganti dengan gambar telanjang, kemudian diganti lagi dengan gambar yang mirip logo PDI-Perjuangan.
(e) Januari 2000, situs yang diserang, antara lain Bursa Efek Jakarta (BEJ), Bank Central Asia dan Indosatnet.

(f) September dan Oktober 2000, Fabian Clone berhasil menjebol web milik Bank Bali, sebelumnya juga berhasil menjebol *web* milik Bank Lippo. Kedua bank itu memberikan layanan *Internet Banking*, kerugian yang diderita lebih besar dibandingkan kerugian yang diderirta BEJ.

(g) Januari 2001, situs milik PT. Ajinomoto Indonesia diserang *craker*. Serangan ini merupakan reaksi atas penggunaan *enzim porcine* (babi) yang digunakan sebagai katalis dalam proses pembuatan bumbu penyedap rasa. Situs Ajinomoto hhtp://www.mjk.ajinomoto.co.id ketika dibuka yang muncul adalah gambar seekor babi yang tengah tersenyum dengan tulisan *Babi, open in December 2K, "Ajinomoto You Lied to Us", "Ajinomoto: HARAM...HARAM...HARAM"*.

(h) Pada 8 Mei 2001, situs Polri mendapat serangan dari Kesatuan Aksi *Hacker* Muslim Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando Jihad.

Bila tidak ditangani dengan baik, ada kemungkinan jumlah kasus berikut korban akan bertambah, baik *cybercrime* dalam bentuk *carding* maupun *deface*, termasuk *cyberporn* meskipun tidak semua publik sepakat bahwa itu adalah suatu kejahatan. Namun, dapat dibayangkan bila orang-orang di sekitar kita, misalnya isteri dan anak kita yang tidak bersalah, tiba-tiba fotonya terpampang di internet dalam keadaan tanpa pakaian dengan teknik rekayasa foto melalui komputer.

Urgensi Penyelesaian "Cybercrime" di Indonesia

Berdasarkan berbagai kasus *cybercrime* yang telah terjadi dan pasti akan bertambah, perlu kiranya dilakukan percepatan dalam menuntaskan kasus *cybercrime*. Untuk menghadapi sekian banyak varian dan modifikasi modus kejahatan di Internet, maka langkah represif dan reaktif yang selama ini dilakukan oleh aparat penegak hukum tidaklah memadai. Aparat tidak siap menghadapinya. Maraknya *cybercrime* menunjukkan ketidakberdayaan pemerintah dalam menyelesaikannya. Oleh karena itu, pemerintah harus meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi, dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*. Aparat kepolisian perlu menanggapi secara serius kejahatan saiber.

Tentunya, harus dibarengi pula dengan serangkaian langkah proaktif dan antisipatif yang dilakukan oleh beragam institusi terkait di Indonesia. Misalnya, asosiasi yang membawahi para *Internet Service Provider* (ISP) dan warnet di Indonesia harus memikirkan langkah yang akan diambil untuk melindungi para konsumen.

Selanjutnya, adalah dengan melakukan kampanye dan edukasi tentang ber-internet yang aman secara komprehensif dan berkala kepada masyarakat umum. Jika hal tersebut tidak segera dilakukan, maka kita harus siap menerima kenyataan bahwa peningkatan penetrasi Internet di Indonesia akan berbanding lurus dengan meningkatnya angka kejahatan Internet secara kuantitatif dan kualitatif. Ujung-ujungnya, hal tersebut justru akan menghancurkan kegiatan usaha/bisnis dan industri internet di Indonesia. Seperti pemblokiran yang dilakukan komunitas internet internasional terhadap pengguna internet dengan nomor *Internet Provider* (IP) Indonesia, sehingga kegiatan bisnis di dunia *cyber* tidak mungkin dilakukan. Itu semua akan menghancurkan kegiatan ekonomi melalui internet.

Tidak kalah pentingnya pula, pemerintah harus bergegas membuat UU *Cyberlaw* untuk menuntaskan kasus *cybercrime*. Perlu dipahami bahwa kegiatan bisnis melalui internet telah mengubah tatanan ekonomi konvesional. Hal itu memunculkan ketidakpastian, karena pihak yang berkomunikasi tidak bertemu secara tatap muka. Untuk memberikan kepastian, perlu dilindungi oleh *cyberlaw*. Meskipun pengguna internet di Indonesia kurang dari 5 % total populasi penduduk (data lainnya menyebutkan hanya 1,9 % atau sekitar 4,38 juta), *cyberlaw* tetap diperlukan sebagai pegangan hukum bagi aparat dalam menuntaskan *cybercrime*. Akan lebih buruk bila tak ada perangkat hukum yang memadai.

Daftar Pustaka

A. Buku

Mahayana, Dimitri. 1999. *Menjemput Masa Depan*, Bandung: PT. Remaja Rosdakarya.

Naisbitt, John, Naisbitt, Nana, & Philips, Douglas. 2001. *High Tech High Touch*. Bandung: Mizan Pustaka.

Piliang, Yasraf Amir. 2001. *Sebuah Dunia yang Menakutkan*. Bandung: Mizan Pustaka.

Raharjo, Agus. 2002. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*. Bandung: Citra Aditya Bakti.

Staubhaar, J. & La Rose, R., *Media Now,* 2000.

Temporal, Paul, K.C. Lee. 2001. *Hi-Tech Hi Touch Branding*. Jakarta: Salemba Empat.

Ustadiyanto, Riyeke. 2001. *Framework e-Commerce*. Yogyakarta: Andi

Wilhelm, Anthony G, *Demokrasi di Era Digital*. 2003. Yogyakarta: Pustaka Pelajar.

B. Sumber lain:

Kompas Cyber Media, 05 Mei 2002.

Republika, 22 Agustus 1999.

komputeraktif, No. 43/18 Desember 2002.

Cybercrime_files\inline_files\SI10.HTM.

Warta Ekonomi.com, 23 Desember 2002.

Terakreditasi Dirjen Dikti SK No. 56/DIKTI/Kep/2005

"Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia

M.E. Fuady

ABSTRACT

It had been long known that technology, as Janus, has two side of coins: the good side, and the bad side. Everybody knows the benefit of technology development. But there aren't much who realize the negative potent of technology. Cybercrime discussed in this article is an example of how crime was developed sophisticatedly by using technological means. Cybercrime, simply defined as criminal acts using cyber and Internet, has faced a new challenge for lawmaker and law enforcement mission. In Indonesia, carding become serious issues to be combated. Another type of cybercrime frequently occur in Indonesia are hacking and deface. Although Internet user in Indonesia is estimated no more than 5% of total population (4.38 million persons), everybody must attended cybercrime issues seriously. The loss of cybercrime reached unspeakable heights and damaged public safety in communication and information flows.

Kata kunci: "cybercrime", realitas virtual, dunia tanpa batas

Internet: Teknologi Pencipta Dunia "Cyber"

Kehadiran teknologi komunikasi modern seperti internet telah membuat pandangan manusia mengenai kehidupan berubah. Paradigma komunikasi manusia dalam menjalani aktivitas ekonomi, bisnis, interaksi sosial, dan politik, menjadi berbeda. Sebelumnya, manusia didominasi oleh aktivitas yang bersifat fisik, *face to face*. Manusia dihalangi oleh berbagai keterbatasan. Dengan internet, ruang, jarak, dan waktu yang membatasi manusia menghilang. Menurut Kenichi Ohmae (Mahayana, 1999:97), itulah dunia tanpa batas (*the borderless world*).

Internet merupakan jaringan dari jutaan komputer yang saling terhubungkan. Dengan internet, setiap orang di seluruh dunia dapat berkomunikasi hanya dengan menekan *keyboard* dan *mouse* di hadapannya. Informasi apa pun yang dibutuhkan telah tersedia. Karena kemudahan yang ditawarkan itulah banyak individu yang menggunakannya. Dibandingkan radio dan televisi, penetrasi internet di kalangan masyarakat, termasuk yang paling cepat. Untuk mencapai pengguna sebanyak 50 juta orang, internet hanya membutuhkan waktu 5 tahun, sementara radio membutuhkan waktu 38 tahun dan televisi 13 tahun (Temporal & Lee, 2002:7). Saat ini, diperkirakan pengguna internet telah mencapai 220 juta orang.

Dengan menggunakan internet, *user* berkesempatan untuk berpetualang, berkelana, berselancar menelusuri *cyberspace*, sebuah dunia komunikasi berbasis komputer (*computer mediated communication*). Realitas yang ditawarkan adalah realitas virtual, kehadirannya tidak dapat ditangkap

atau dipegang tangan, tetapi dikonstruksikan secara sosial oleh orang-orang yang menggeluti teknologi komunikasi dan informasi. Realitas *cyberspace* adalah kenyataan yang melampaui dan artifisial (*hyperreal*). Menurut Piliang (2001), karena rekayasa sedemikian rupa, kenyataan (*real*) ditutupi oleh tanda kenyataan (*sign of real*) sedemikian rupa, sehingga antara tanda dan relitas, antara model dan kenyataan, tidak lagi dapat dibedakan.

Cyberspace menawarkan segala hal yang diperlukan manusia, termasuk kesenangan, keuntungan, dan kemudahan tanpa bersusah payah menggerakkan badan untuk memeroleh sesuatu. Berbagai informasi gratis dari surat kabar dalam dan luar negeri dapat diperoleh tanpa membeli. Menikmati musik tanpa harus membeli kaset. Bagi dosen, berbagai literatur tersaji secara gratis tanpa harus pergi ke tempat berada. Inilah "zona mabuk teknologi" yang dikemukakan Philips dan Naisbitt (2001).

Kehidupan virtual yang disajikan *cyberspace* telah memunculkan bentuk aktivitas baru untuk mencapai kepuasan, seperti *teleshopping*, *teleconference*, *virtual gallery*, *virtual museum*, *e-commerce*, namun juga memunculkan penyimpangan-penyimpangan seperti kejahatan dengan memanfaatkan internet atau *cybercrime*.

"Cybercrime": Bentuk Kejahatan di Dunia Maya

Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime. The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai:"…*any illegal act requiring knowledge of 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*". Hamzah (1989) mengartikan: "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dari beberapa pengertian di atas, Wisnubroto (1999) merumuskan *computer crime* sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas, *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih. Selanjutnya, disebabkan kejahatan itu dilakukan di ruang *cyber* melalui internet, muncul istilah *cybercrime*.

Bagi sebagian besar masyarakat yang terbiasa menggunakan media teknologi komunikasi (telekomunikasi), *cybercrime* bukanlah istilah yang asing terdengar. *Cybercrime* atau kejahatan di ruang maya merupakan sebuah fenomena yang tidak terbantahkan. Tidak terlihat namun nyata. Terdapat berbagai kasus *cybercrime* yang kian hari kian meningkat, terutama di negara-negara yang tidak memiliki kepastian hukum dalam bidang teknologi komunikasi modern (*convergence*).

Teknologi komunikasi yang memiliki kekuatan dahsyat dalam merubah perilaku komunikasi manusia, selain membawa keuntungan berupa kemudahan dalam berkomunikasi, ternyata memiliki "sisi gelap". Teknologi membawa kerugian, salah satunya berupa semakin dipermudahkannya "penjahat" dalam melakukan kejahatannya. Kecanggihan teknologi memungkinkan penjahat *cyber* memangsa korban-korbannya. Meski tidak mau disebut sebagai pelaku kriminal, sebagai akibat dari perbuatannya, mereka tidak ada bedanya dengan seorang penjahat.

Menurut Raharjo (2002:29), sebagai sebuah gejala sosial, kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern). Kejahatan konvensional di dunia nyata muncul dalam dunia maya (*virtual*) dengan wajah kejahatan yang telah diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau *cybercrime* membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, tidak merasakannya sebagai sebuah bentuk kejahatan. Padahal, sudah begitu banyak korban (*victim*) dan

kerugian moril dan materil akibat *cybercrime*. Korbannya dapat berupa *netizen* (penduduk dunia *virtual*/penghuni *cyberspace*) dan masyarakat luas yang awam.

Perusahaan yang bergerak dalam bidang bisnis dan individu tak berdosa, yang tidak memiliki keahlian bahkan pemahaman akan teknologi komunikasi, dapat menjadi korban. Tidak perlu jauh-jauh, kita semua masih ingat dengan kasus mahasiswa dan artis "bugil" yang beredar di internet. Sedikit sekali di antara mereka yang memahami teknologi komunikasi, tetapi mereka telah menjadi korban. Sebut saja artis dengan inisial YS, KD, KF, CK, dan masih banyak lagi. Itu salah satu contoh kecil korban dari *cybercrime*. Meski memang ada publik yang tidak menyepakati *cyberporn* sebagai *cybercrime*. Tetapi, kita telah melihat adanya korban akibat perbuatan pelaku *cybercrime*. Sebagai catatan penting, menurut Menteri Negara Komunikasi dan Informasi, sekitar 50 persen kalangan muda yang menggunakan internet lebih suka untuk mengunjungi situs porno (*Kompas Cyber Media*, 05 Mei 2002).

Untuk memahami *cybercrime*, perlu kiranya dipahami terlebih dahulu apa yang disebut dengan *hacker*, *cracker* dan beberapa lainnya. Karena, seperti halnya kehidupan nyata, ada di antara mereka yang "hitam" dan "putih", ada yang berlaku seperti pahlawan dan penjahat.

(1) *Hacker*

Hacker secara harfiah berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup melalui komputer ke dalam jaringan komputer (*Republika*, 22 Agustus 1999). Menurut Ustadiyanto (2001:304), ada definisi yang relevan, yakni *hacker* adalah orang-orang yang ahli dalam bidangnya. Bila komputer, maka dia pandai menggunakannya. Ia sangat menguasai komputer. *Hacker* adalah orang-orang yang gemar mempelajari seluk-beluk sistem komputer dan bereksperimen dengannya. Mereka pandai untuk menyusup ke dalam jaringan komunikasi suatu institusi di dunia maya. *Hacker* menjunjung tinggi etika atau norma yang berlaku di dunia maya. Mereka anti penyensoran, anti penipuan, dan pemaksaan kehendak pada orang lain. Mereka memegang prinsip bahwa meng-*hack* untuk tujuan meningkatkan keamanan jaringan internet. Misalnya, bila ada sebuah perusahaan perbankan mengatakan bahwa jaringan sistem komunikasi mereka sudah sangat canggih dan mustahil dibobol, tidak dapat ditembus oleh siapa pun, maka *hacker* tertantang untuk mencoba dan setelah berhasil mereka memperingatkan betapa lemahnya sistem informasi perusahaan terrsebut. Oleh karena itu, tidak sedikit dari mereka yang akhirnya direkrut perusahaan untuk mengamankan sistem informasi dan komunikasi di dunia maya.

(2) *Cracker*

Di dunia *cyber*, ada pula *hacker* yang memiki sisi gelap. Mereka disebut *cracker*. Para *cracker* ini secara ilegal melakukan penyusupan dan perusakan terhadap situs, *website,* dan sistem keamanan jaringan internet untuk memperoleh kesenangan dan keuntungan. Mereka bangga dan sombong atas keberhasilan mereka merusak situs sebuah perusahaan. Serangannya sangat luar biasa. Kementerian Petahanan Amerika Serikat di Pentagon mencatat serangan 100 *cracker* dalam satu hari (*Republika*, 6 Januari 2000).

(3) *Carder*

Carder adalah orang yang melakukan *cracking*, yakni pembobolan terhadap kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk kepentingan pribadi. Biasanya yang menjadi korbannya adalah mereka yang memiliki kartu kredit dalam jumlah besar. Menurut hasil riset, pada tahun 2002, Indonesia menempati urutan kedua setelah Ukraina dalam kejahatan *carding*.

(4) *Deface*

Deface adalah tindakan menyusup ke suatu situs, lalu mengubah tampilan halaman dari situs dengan tujuan tertentu. Indonesia pernah diserang para *deface* yang mengubah situs TNI. Tampilan gambar Burung Garuda Pancasila diganti dengan lambang palu arit. *Hompage* Polri diganti tampilannya dengan

gambar wanita telanjang.

(5) *Phreaker*
*Yaitu ses*eorang yang melakukan *cracking* terhadap jaringan telepon, sehingga dapat menelepon secara gratis ke daerah manapun yang dituju (*Komputeraktif*, No. 43/18 Desember 2002). Di Indonesia, kasus semacam ini pernah terjadi pada wartel–wartel.

Para pelaku *hacking* biasanya bukan dari kalangan lapisan bawah, pada umumnya mereka adalah kaum terpelajar, setidak-tidaknya mengenyam pendidikan formal sampai tingkat tertentu dan dapat menggunakan atau mengoperasikan komputer. Para *craker* adalah orang yang berpendidikan, tidak buta teknologi, secara ekonomis mampu dan tidak termasuk dalam masyarakat lapisan bawah. Kejahatan ini dapat dikategorikan kepada *white collar crime* (kejahatan kerah putih). Jo Ann L. Miller, mengkategorikan pelakunya menjadi 4 (empat).

(a) *Organizational occupational crime*
Pelakunya adalah para eksekutif. Mereka melakukan perbuatan ilegal atau merugikan orang lain melalui jaringan internet demi kepentingan atau keuntungan korporasi.

(b) *Government occupational crime*
Pelakunya adalah pejabat atau birokrat yang melakukan perbuatan ilegal melalui internet atas persetujuan atau perintah negara atau pemerintah, meski dalam banyak kasus, bila terungkap hal itu akan disangkal.

(c) *Professional occupational crime*
Berbagai profesi yang melakukan kejahatan secara sengaja (*malpractice*).

(d) *Individual occupational crime*
Perilaku menyimpang yang dilakukan oleh para pengusaha, pemilik modal atau orang-orang independen lainnya, walau mungkin tidak tinggi tingkat sosial ekonominya. Dalam bidang kerjanya kalangan ini memilih jalan yang menyimpang yang melanggar hukum atau merugikan orang lain.

Karakteristik "Cybercrime"

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain (CYBERCRIME_files\ inline_files\ SI10.HTM):

(1) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/ wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.

(2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.

(3) Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional

(4) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya

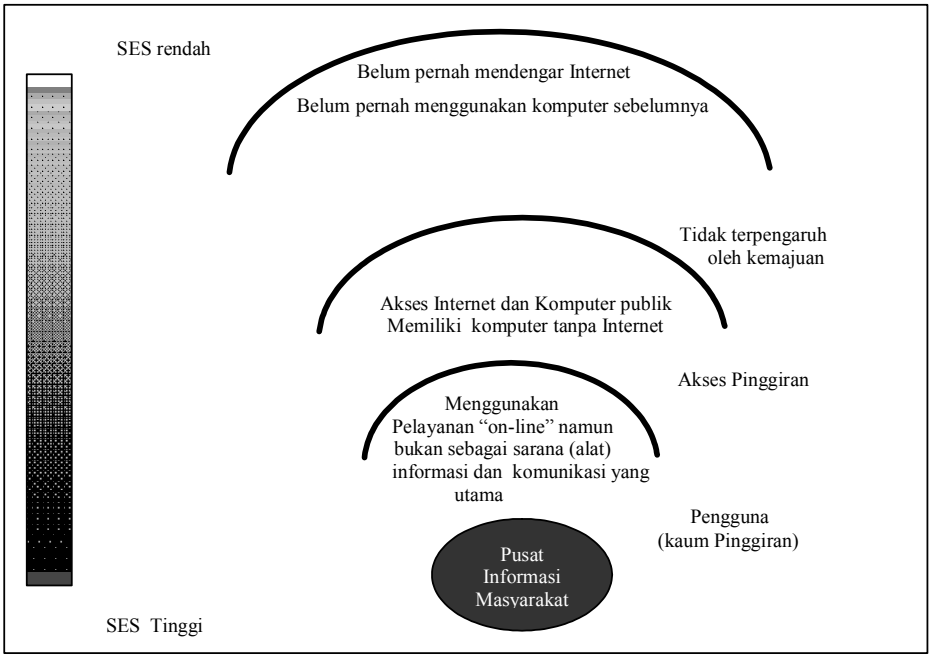
(5) Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

"Cybercrime" di Indonesia

Di antara negara berkembang, Indonesia termasuk negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia tidak memrioritaskan strategi pengembangan dan penguasaan teknologi. Yang terjadi kemudian, transfer teknologi dari negara maju tidak serta merta diikuti dengan penguasaan teknologi oleh negara berkembang seperti Indonesia. Bandingkan saja dengan Malaysia yang telah memproduksi secara massal *software*, per*sonal Computer* (PC), dan ponsel. Sungguh ironis memang, karena menjelang 1980-an Indonesia adalah negara Asia Tenggara pertama yang memiliki satelit komunikasi. Singapura dan Malaysia yang saat itu masih menyewa satelit Palapa dari Indonesia, kini menjadi negara maju berbasis teknologi komunikasi modern.

Meski masih diperdebatkan, dapat dikatakan Indonesia merupakan negara yang memiliki kesenjangan digital yang cukup lebar. Kesenjangan digital dapat diartikan sebagai adanya jurang di antara mereka yang mampu mengakses teknologi komunikasi dan yang tidak mampu (Staubhaar & La Rose, 2000:9). Selain masih senjangnya tingkat pendidikan dan ekonomi di Indonesia, kesempatan

Gambar 1: Model Pusat-Pinggiran Akses Teleteknologi



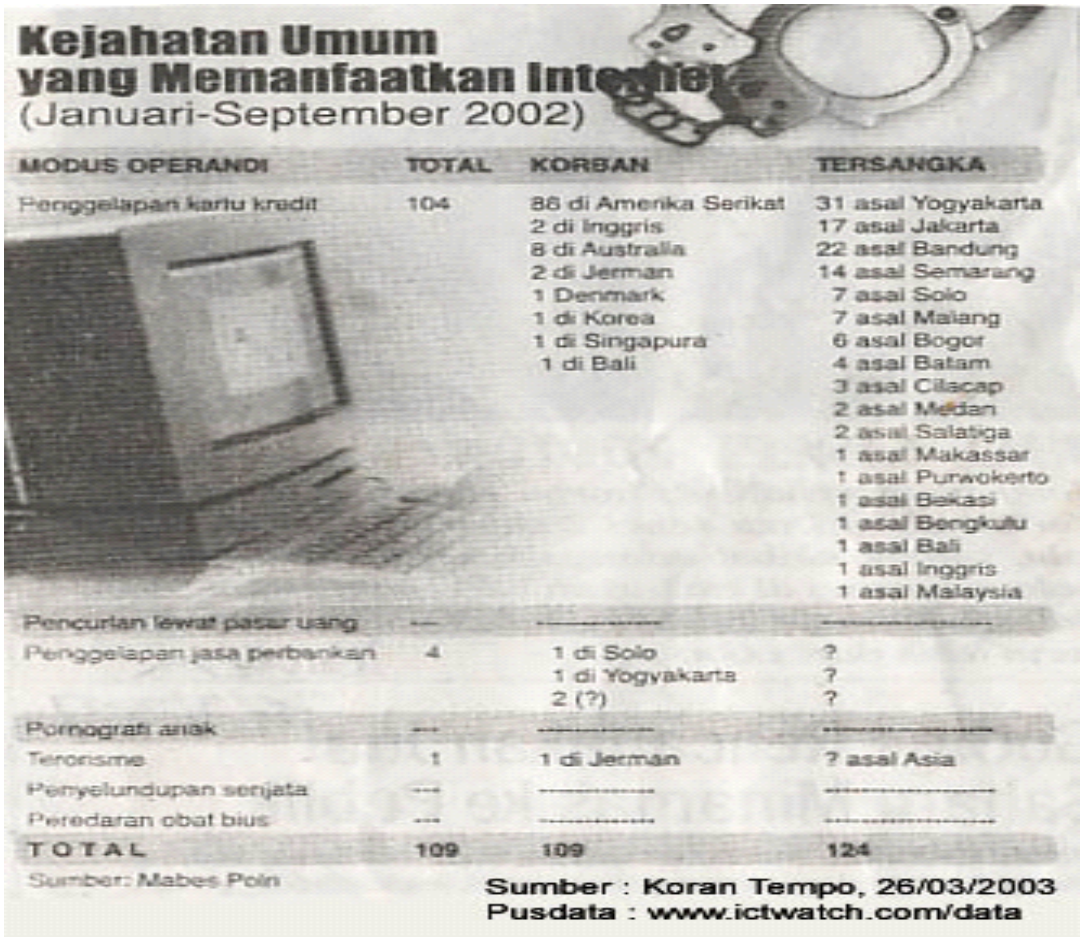
Sumber: Wilhelm (2003:119)

untuk menggunakan teknologi komunikasi di Indonesia belum merata. Ketimpangan, ketidakmilikan informasi dan telekomunikasi dapat dibagi dalam beberapa kategori. Yang paling banyak aksesnya, tentu saja, yang paling dekat dengan pusat informasi masyarakat.

Meskipun terdapat kesenjangan digital, di Indonesia marak sekali kejahatan *cyber*. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para *hacker* hitam. Mereka bisa memperoleh barang apa pun yang diinginkan, mulai dari berlian, radar laut, *corporate software*, *computer server*, Harley Davidson, hingga senjata M-16 (*Warta Ekonomi.com*, 23 Desember 2002) dengan menggunakan kartu kredit milik orang lain. Istilahnya adalah c*arding*. Para *carder* (*hacker* hitam) memesan barang-barang melalui internet untuk dikirimkan ke negara mereka berada. Barang yang dipesan dapat digunakan sendiri, dapat pula dijual dengan harga yang sangat murah. Misalnya, *Notebook* bermerk *Sony* seharga 20 Juta yang dipesan melalui *carding*, dijual seharga 4 Juta rupiah. Untuk yang satu ini, *ClearCommerce*, perusahaan keamanan internet yang berbasis di Texas, Amerika Serikat, memasukkan Indonesia ke dalam daftar negara-negara terburuk untuk kejahatan yang memanfaatkan kecanggihan teknologi komunikasi. Setidaknya, 20 persen transaksi kartu kredit internet yang berasal dari Indonesia merupakan penipuan. Berikut ini adalah data kejahatan yang memanfaatkan internet:

Dari data di bawah (*Koran Tempo*, 26 Maret 2003), Yogyakarta menempati urutan pertama dan Bandung kedua dalam *cybercrime* jenis *carding di* Indonesia. Yang melakukan jenis kejahatan itu adalah kalangan muda, biasanya mahasiswa. Seorang mahasiswa universitas swasta di Bandung pernah memesan 5 buah ponsel *Nokia Communicator* yang ia jual seharga 5 Juta rupiah, padahal saat itu harganya berkisar 10 Juta rupiah.

Gambar 2: Kejahatan Umum yang Memanfaatkan Internet



Kejahatan Umum yang Memanfaatkan Internet
(Januari-September 2002)

MODUS OPERANDI	TOTAL	KORBAN	TERSANGKA
Penggelapan kartu kredit	104	86 di Amerika Serikat 2 di Inggris 8 di Australia 2 di Jerman 1 Denmark 1 di Korea 1 di Singapura 1 di Bali	31 asal Yogyakarta 17 asal Jakarta 22 asal Bandung 14 asal Semarang 7 asal Solo 7 asal Malang 6 asal Bogor 4 asal Batam 3 asal Cilacap 2 asal Medan 2 asal Salatiga 1 asal Makassar 1 asal Purwokerto 1 asal Bekasi 1 asal Bengkulu 1 asal Bali 1 asal Inggris 1 asal Malaysia
Pencurian lewat pasar uang	---	----------	----------
Penggelapan jasa perbankan	4	1 di Solo 1 di Yogyakarta 2 (?)	? ? ?
Pornografi anak	---	----------	----------
Terorisme	1	1 di Jerman	? asal Asia
Penyelundupan senjata	---	----------	----------
Peredaran obat bius	---	----------	----------
TOTAL	109	109	124

Sumber: Mabes Polri

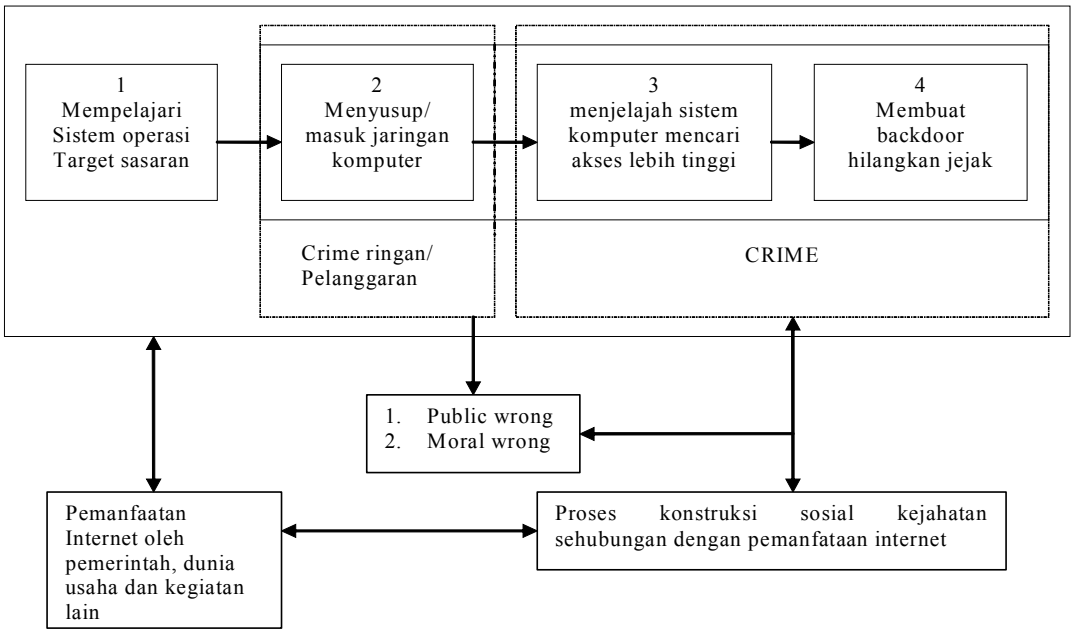
Sumber : Koran Tempo, 26/03/2003
Pusdata : www.ictwatch.com/data

Agar tidak diketahui identitasnya, ia melakukan *carding* di warnet sekitar kampus dan saat mengambil pesanan, agar dimudahkan, ia bekerjasama dan memberi sejumlah uang kepada oknum karyawan biro pengiriman paket terkemuka di Indonesia.

Indonesia tampaknya akan semakin mengukuhkan diri sebagai negara kampiun penipuan kartu kredit di internet Dalam berbagai urusan yang berkonotasi buruk, Indonesia memang seringkali termasuk di dalamnya, mulai dari pendapatan perkapita yang rendah, mutu pendidikan, tingkat korupsi, termasuk *cybercrime* jenis *carding*.

Kejahatan memang tidak dapat diprediksi kejadiannya, tidak mempedulikan tempat dan suasana ketika hendak muncul, tidak pula membanding-bandingkan siapa pelaku dan korbannya, tidak mengenal kasta ataupun status sosial pelaku dan korbannya. Saat muncul, ia dapat menjadi bahan yang menarik untuk dibicarakan, baik di media massa maupun ruang-ruang seminar. Apalagi saat kejahatan itu dipadukan dengan kecanggihan teknologi komunikasi. Tanpa sadar

Gambar 3. Bagan Konstruksi Kejahatan dari "Hacking"



Sumber: Raharjo (2002)

di sekeliling kita terdapat kejahatan yang "*innocent*", seolah tanpa dosa dan begitu halus.

Adapun konstruksi kejahatan *Hacking* dapat dilihat pada gambar 3.

Selain *cybercrime* jenis *carding*, di Indonesia juga sering terjadi kasus *deface*. Tampilan situs di Internet dirusak dan diganti oleh para *hacker* hitam. Berikut ini adalah kasus-kasus yang pernah terjadi (Raharjo, 202:35):

(a) Tahun 1997 ketika masalah Timor-Timur menghangat, situs milik Departemen Luar Negri dan ABRI (TNI, pen) dijebol oleh *craker Porto* (Portugis) yang pro-kemerdekaan. Mereka juga merusak situs-situs bisnis dan pendidikan. Serangan dari *craker* Porto ini mendapat balasan dari *craker* Indonesia. Hal ini dilakukan karena, menurut mereka, *craker* Porto dinilai keterlaluan, serangannya membabi-buta, tidak mempedulikan apakah itu situs milik pemerintah ataupun bukan, situs bisnis maupun situs pendidikan.
(b) Tahun 1998, tampilan depan atau *frontpage* Pusat Dokumentasi Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) diganti dengan gambar wanita telanjang.
(c) Tahun 1998, setelah kerusuhan 13–14 Mei, *craker* yang diduga berasal dari Cina menghantam situs milik pemerintah, yaitu BKKBN. Serangan ini merupakan reaksi atas pemberitaan media mengenai kerusuhan Mei yang menyebabkan etnis Cina di Indonesia menjadi korban pembantaian dan pemerkosaan.
(d) Juni 1999, *homepage* POLRI diganti dengan gambar telanjang, kemudian diganti lagi dengan gambar yang mirip logo PDI-Perjuangan.
(e) Januari 2000, situs yang diserang, antara lain Bursa Efek Jakarta (BEJ), Bank Central Asia dan Indosatnet.

(f) September dan Oktober 2000, Fabian Clone berhasil menjebol web milik Bank Bali, sebelumnya juga berhasil menjebol *web* milik Bank Lippo. Kedua bank itu memberikan layanan *Internet Banking*, kerugian yang diderita lebih besar dibandingkan kerugian yang diderirta BEJ.

(g) Januari 2001, situs milik PT. Ajinomoto Indonesia diserang *craker*. Serangan ini merupakan reaksi atas penggunaan *enzim porcine* (babi) yang digunakan sebagai katalis dalam proses pembuatan bumbu penyedap rasa. Situs Ajinomoto hhtp://www.mjk.ajinomoto.co.id ketika dibuka yang muncul adalah gambar seekor babi yang tengah tersenyum dengan tulisan *Babi, open in December 2K, "Ajinomoto You Lied to Us", "Ajinomoto: HARAM...HARAM...HARAM"*.

(h) Pada 8 Mei 2001, situs Polri mendapat serangan dari Kesatuan Aksi *Hacker* Muslim Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando Jihad.

Bila tidak ditangani dengan baik, ada kemungkinan jumlah kasus berikut korban akan bertambah, baik *cybercrime* dalam bentuk *carding* maupun *deface*, termasuk *cyberporn* meskipun tidak semua publik sepakat bahwa itu adalah suatu kejahatan. Namun, dapat dibayangkan bila orang-orang di sekitar kita, misalnya isteri dan anak kita yang tidak bersalah, tiba-tiba fotonya terpampang di internet dalam keadaan tanpa pakaian dengan teknik rekayasa foto melalui komputer.

Urgensi Penyelesaian "Cybercrime" di Indonesia

Berdasarkan berbagai kasus *cybercrime* yang telah terjadi dan pasti akan bertambah, perlu kiranya dilakukan percepatan dalam menuntaskan kasus *cybercrime*. Untuk menghadapi sekian banyak varian dan modifikasi modus kejahatan di Internet, maka langkah represif dan reaktif yang selama ini dilakukan oleh aparat penegak hukum tidaklah memadai. Aparat tidak siap menghadapinya. Maraknya *cybercrime* menunjukkan ketidakberdayaan pemerintah dalam menyelesaikannya. Oleh karena itu, pemerintah harus meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi, dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*. Aparat kepolisian perlu menanggapi secara serius kejahatan saiber.

Tentunya, harus dibarengi pula dengan serangkaian langkah proaktif dan antisipatif yang dilakukan oleh beragam institusi terkait di Indonesia. Misalnya, asosiasi yang membawahi para *Internet Service Provider* (ISP) dan warnet di Indonesia harus memikirkan langkah yang akan diambil untuk melindungi para konsumen.

Selanjutnya, adalah dengan melakukan kampanye dan edukasi tentang ber-internet yang aman secara komprehensif dan berkala kepada masyarakat umum. Jika hal tersebut tidak segera dilakukan, maka kita harus siap menerima kenyataan bahwa peningkatan penetrasi Internet di Indonesia akan berbanding lurus dengan meningkatnya angka kejahatan Internet secara kuantitatif dan kualitatif. Ujung-ujungnya, hal tersebut justru akan menghancurkan kegiatan usaha/bisnis dan industri internet di Indonesia. Seperti pemblokiran yang dilakukan komunitas internet internasional terhadap pengguna internet dengan nomor *Internet Provider* (IP) Indonesia, sehingga kegiatan bisnis di dunia *cyber* tidak mungkin dilakukan. Itu semua akan menghancurkan kegiatan ekonomi melalui internet.

Tidak kalah pentingnya pula, pemerintah harus bergegas membuat UU *Cyberlaw* untuk menuntaskan kasus *cybercrime*. Perlu dipahami bahwa kegiatan bisnis melalui internet telah mengubah tatanan ekonomi konvesional. Hal itu memunculkan ketidakpastian, karena pihak yang berkomunikasi tidak bertemu secara tatap muka. Untuk memberikan kepastian, perlu dilindungi oleh *cyberlaw*. Meskipun pengguna internet di Indonesia kurang dari 5 % total populasi penduduk (data lainnya menyebutkan hanya 1,9 % atau sekitar 4,38 juta), *cyberlaw* tetap diperlukan sebagai pegangan hukum bagi aparat dalam menuntaskan *cybercrime*. Akan lebih buruk bila tak ada perangkat hukum yang memadai.

Daftar Pustaka

A. Buku

Mahayana, Dimitri. 1999. *Menjemput Masa Depan*, Bandung: PT. Remaja Rosdakarya.

Naisbitt, John, Naisbitt, Nana, & Philips, Douglas. 2001. *High Tech High Touch*. Bandung: Mizan Pustaka.

Piliang, Yasraf Amir. 2001. *Sebuah Dunia yang Menakutkan*. Bandung: Mizan Pustaka.

Raharjo, Agus. 2002. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*. Bandung: Citra Aditya Bakti.

Staubhaar, J. & La Rose, R., *Media Now,* 2000.

Temporal, Paul, K.C. Lee. 2001. *Hi-Tech Hi Touch Branding*. Jakarta: Salemba Empat.

Ustadiyanto, Riyeke. 2001. *Framework e-Commerce*. Yogyakarta: Andi

Wilhelm, Anthony G, *Demokrasi di Era Digital*. 2003. Yogyakarta: Pustaka Pelajar.

B. Sumber lain:

Kompas Cyber Media, 05 Mei 2002.

Republika, 22 Agustus 1999.

komputeraktif, No. 43/18 Desember 2002.

Cybercrime_files\inline_files\SI10.HTM.

Warta Ekonomi.com, 23 Desember 2002.

Terakreditasi Dirjen Dikti SK No. 56/DIKTI/Kep/2005

"Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia

M.E. Fuady

ABSTRACT

It had been long known that technology, as Janus, has two side of coins: the good side, and the bad side. Everybody knows the benefit of technology development. But there aren't much who realize the negative potent of technology. Cybercrime discussed in this article is an example of how crime was developed sophisticatedly by using technological means. Cybercrime, simply defined as criminal acts using cyber and Internet, has faced a new challenge for lawmaker and law enforcement mission. In Indonesia, carding become serious issues to be combated. Another type of cybercrime frequently occur in Indonesia are hacking and deface. Although Internet user in Indonesia is estimated no more than 5% of total population (4.38 million persons), everybody must attended cybercrime issues seriously. The loss of cybercrime reached unspeakable heights and damaged public safety in communication and information flows.

Kata kunci: "cybercrime", realitas virtual, dunia tanpa batas

Internet: Teknologi Pencipta Dunia "Cyber"

Kehadiran teknologi komunikasi modern seperti internet telah membuat pandangan manusia mengenai kehidupan berubah. Paradigma komunikasi manusia dalam menjalani aktivitas ekonomi, bisnis, interaksi sosial, dan politik, menjadi berbeda. Sebelumnya, manusia didominasi oleh aktivitas yang bersifat fisik, *face to face*. Manusia dihalangi oleh berbagai keterbatasan. Dengan internet, ruang, jarak, dan waktu yang membatasi manusia menghilang. Menurut Kenichi Ohmae (Mahayana, 1999:97), itulah dunia tanpa batas (*the borderless world*).

Internet merupakan jaringan dari jutaan komputer yang saling terhubungkan. Dengan internet, setiap orang di seluruh dunia dapat berkomunikasi hanya dengan menekan *keyboard* dan *mouse* di hadapannya. Informasi apa pun yang dibutuhkan telah tersedia. Karena kemudahan yang ditawarkan itulah banyak individu yang menggunakannya. Dibandingkan radio dan televisi, penetrasi internet di kalangan masyarakat, termasuk yang paling cepat. Untuk mencapai pengguna sebanyak 50 juta orang, internet hanya membutuhkan waktu 5 tahun, sementara radio membutuhkan waktu 38 tahun dan televisi 13 tahun (Temporal & Lee, 2002:7). Saat ini, diperkirakan pengguna internet telah mencapai 220 juta orang.

Dengan menggunakan internet, *user* berkesempatan untuk berpetualang, berkelana, berselancar menelusuri *cyberspace*, sebuah dunia komunikasi berbasis komputer (*computer mediated communication*). Realitas yang ditawarkan adalah realitas virtual, kehadirannya tidak dapat ditangkap

atau dipegang tangan, tetapi dikonstruksikan secara sosial oleh orang-orang yang menggeluti teknologi komunikasi dan informasi. Realitas *cyberspace* adalah kenyataan yang melampaui dan artifisial (*hyperreal*). Menurut Piliang (2001), karena rekayasa sedemikian rupa, kenyataan (*real*) ditutupi oleh tanda kenyataan (*sign of real*) sedemikian rupa, sehingga antara tanda dan relitas, antara model dan kenyataan, tidak lagi dapat dibedakan.

Cyberspace menawarkan segala hal yang diperlukan manusia, termasuk kesenangan, keuntungan, dan kemudahan tanpa bersusah payah menggerakkan badan untuk memeroleh sesuatu. Berbagai informasi gratis dari surat kabar dalam dan luar negeri dapat diperoleh tanpa membeli. Menikmati musik tanpa harus membeli kaset. Bagi dosen, berbagai literatur tersaji secara gratis tanpa harus pergi ke tempat berada. Inilah "zona mabuk teknologi" yang dikemukakan Philips dan Naisbitt (2001).

Kehidupan virtual yang disajikan *cyberspace* telah memunculkan bentuk aktivitas baru untuk mencapai kepuasan, seperti *teleshopping*, *teleconference*, *virtual gallery*, *virtual museum*, *e-commerce*, namun juga memunculkan penyimpangan-penyimpangan seperti kejahatan dengan memanfaatkan internet atau *cybercrime*.

"Cybercrime": Bentuk Kejahatan di Dunia Maya

Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime. The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai:"…*any illegal act requiring knowledge of 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*". Hamzah (1989) mengartikan: "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dari beberapa pengertian di atas, Wisnubroto (1999) merumuskan *computer crime* sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas, *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih. Selanjutnya, disebabkan kejahatan itu dilakukan di ruang *cyber* melalui internet, muncul istilah *cybercrime*.

Bagi sebagian besar masyarakat yang terbiasa menggunakan media teknologi komunikasi (telekomunikasi), *cybercrime* bukanlah istilah yang asing terdengar. *Cybercrime* atau kejahatan di ruang maya merupakan sebuah fenomena yang tidak terbantahkan. Tidak terlihat namun nyata. Terdapat berbagai kasus *cybercrime* yang kian hari kian meningkat, terutama di negara-negara yang tidak memiliki kepastian hukum dalam bidang teknologi komunikasi modern (*convergence*).

Teknologi komunikasi yang memiliki kekuatan dahsyat dalam merubah perilaku komunikasi manusia, selain membawa keuntungan berupa kemudahan dalam berkomunikasi, ternyata memiliki "sisi gelap". Teknologi membawa kerugian, salah satunya berupa semakin dipermudahkannya "penjahat" dalam melakukan kejahatannya. Kecanggihan teknologi memungkinkan penjahat *cyber* memangsa korban-korbannya. Meski tidak mau disebut sebagai pelaku kriminal, sebagai akibat dari perbuatannya, mereka tidak ada bedanya dengan seorang penjahat.

Menurut Raharjo (2002:29), sebagai sebuah gejala sosial, kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern). Kejahatan konvensional di dunia nyata muncul dalam dunia maya (*virtual*) dengan wajah kejahatan yang telah diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau *cybercrime* membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, tidak merasakannya sebagai sebuah bentuk kejahatan. Padahal, sudah begitu banyak korban (*victim*) dan

kerugian moril dan materil akibat *cybercrime*. Korbannya dapat berupa *netizen* (penduduk dunia *virtual*/penghuni *cyberspace*) dan masyarakat luas yang awam.

Perusahaan yang bergerak dalam bidang bisnis dan individu tak berdosa, yang tidak memiliki keahlian bahkan pemahaman akan teknologi komunikasi, dapat menjadi korban. Tidak perlu jauh-jauh, kita semua masih ingat dengan kasus mahasiswa dan artis "bugil" yang beredar di internet. Sedikit sekali di antara mereka yang memahami teknologi komunikasi, tetapi mereka telah menjadi korban. Sebut saja artis dengan inisial YS, KD, KF, CK, dan masih banyak lagi. Itu salah satu contoh kecil korban dari *cybercrime*. Meski memang ada publik yang tidak menyepakati *cyberporn* sebagai *cybercrime*. Tetapi, kita telah melihat adanya korban akibat perbuatan pelaku *cybercrime*. Sebagai catatan penting, menurut Menteri Negara Komunikasi dan Informasi, sekitar 50 persen kalangan muda yang menggunakan internet lebih suka untuk mengunjungi situs porno (*Kompas Cyber Media*, 05 Mei 2002).

Untuk memahami *cybercrime*, perlu kiranya dipahami terlebih dahulu apa yang disebut dengan *hacker*, *cracker* dan beberapa lainnya. Karena, seperti halnya kehidupan nyata, ada di antara mereka yang "hitam" dan "putih", ada yang berlaku seperti pahlawan dan penjahat.

(1) *Hacker*

Hacker secara harfiah berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup melalui komputer ke dalam jaringan komputer (*Republika*, 22 Agustus 1999). Menurut Ustadiyanto (2001:304), ada definisi yang relevan, yakni *hacker* adalah orang-orang yang ahli dalam bidangnya. Bila komputer, maka dia pandai menggunakannya. Ia sangat menguasai komputer. *Hacker* adalah orang-orang yang gemar mempelajari seluk-beluk sistem komputer dan bereksperimen dengannya. Mereka pandai untuk menyusup ke dalam jaringan komunikasi suatu institusi di dunia maya. *Hacker* menjunjung tinggi etika atau norma yang berlaku di dunia maya. Mereka anti penyensoran, anti penipuan, dan pemaksaan kehendak pada orang lain. Mereka memegang prinsip bahwa meng-*hack* untuk tujuan meningkatkan keamanan jaringan internet. Misalnya, bila ada sebuah perusahaan perbankan mengatakan bahwa jaringan sistem komunikasi mereka sudah sangat canggih dan mustahil dibobol, tidak dapat ditembus oleh siapa pun, maka *hacker* tertantang untuk mencoba dan setelah berhasil mereka memperingatkan betapa lemahnya sistem informasi perusahaan terrsebut. Oleh karena itu, tidak sedikit dari mereka yang akhirnya direkrut perusahaan untuk mengamankan sistem informasi dan komunikasi di dunia maya.

(2) *Cracker*

Di dunia *cyber*, ada pula *hacker* yang memiki sisi gelap. Mereka disebut *cracker*. Para *cracker* ini secara ilegal melakukan penyusupan dan perusakan terhadap situs, *website,* dan sistem keamanan jaringan internet untuk memperoleh kesenangan dan keuntungan. Mereka bangga dan sombong atas keberhasilan mereka merusak situs sebuah perusahaan. Serangannya sangat luar biasa. Kementerian Petahanan Amerika Serikat di Pentagon mencatat serangan 100 *cracker* dalam satu hari (*Republika*, 6 Januari 2000).

(3) *Carder*

Carder adalah orang yang melakukan *cracking*, yakni pembobolan terhadap kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk kepentingan pribadi. Biasanya yang menjadi korbannya adalah mereka yang memiliki kartu kredit dalam jumlah besar. Menurut hasil riset, pada tahun 2002, Indonesia menempati urutan kedua setelah Ukraina dalam kejahatan *carding*.

(4) *Deface*

Deface adalah tindakan menyusup ke suatu situs, lalu mengubah tampilan halaman dari situs dengan tujuan tertentu. Indonesia pernah diserang para *deface* yang mengubah situs TNI. Tampilan gambar Burung Garuda Pancasila diganti dengan lambang palu arit. *Hompage* Polri diganti tampilannya dengan

gambar wanita telanjang.

(5) *Phreaker*
*Yaitu ses*eorang yang melakukan *cracking* terhadap jaringan telepon, sehingga dapat menelepon secara gratis ke daerah manapun yang dituju (*Komputeraktif*, No. 43/18 Desember 2002). Di Indonesia, kasus semacam ini pernah terjadi pada wartel–wartel.

Para pelaku *hacking* biasanya bukan dari kalangan lapisan bawah, pada umumnya mereka adalah kaum terpelajar, setidak-tidaknya mengenyam pendidikan formal sampai tingkat tertentu dan dapat menggunakan atau mengoperasikan komputer. Para *craker* adalah orang yang berpendidikan, tidak buta teknologi, secara ekonomis mampu dan tidak termasuk dalam masyarakat lapisan bawah. Kejahatan ini dapat dikategorikan kepada *white collar crime* (kejahatan kerah putih). Jo Ann L. Miller, mengkategorikan pelakunya menjadi 4 (empat).

(a) *Organizational occupational crime*
Pelakunya adalah para eksekutif. Mereka melakukan perbuatan ilegal atau merugikan orang lain melalui jaringan internet demi kepentingan atau keuntungan korporasi.

(b) *Government occupational crime*
Pelakunya adalah pejabat atau birokrat yang melakukan perbuatan ilegal melalui internet atas persetujuan atau perintah negara atau pemerintah, meski dalam banyak kasus, bila terungkap hal itu akan disangkal.

(c) *Professional occupational crime*
Berbagai profesi yang melakukan kejahatan secara sengaja (*malpractice*).

(d) *Individual occupational crime*
Perilaku menyimpang yang dilakukan oleh para pengusaha, pemilik modal atau orang-orang independen lainnya, walau mungkin tidak tinggi tingkat sosial ekonominya. Dalam bidang kerjanya kalangan ini memilih jalan yang menyimpang yang melanggar hukum atau merugikan orang lain.

Karakteristik "Cybercrime"

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain (CYBERCRIME_files\ inline_files\ SI10.HTM):

(1) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/ wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.

(2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.

(3) Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional

(4) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya

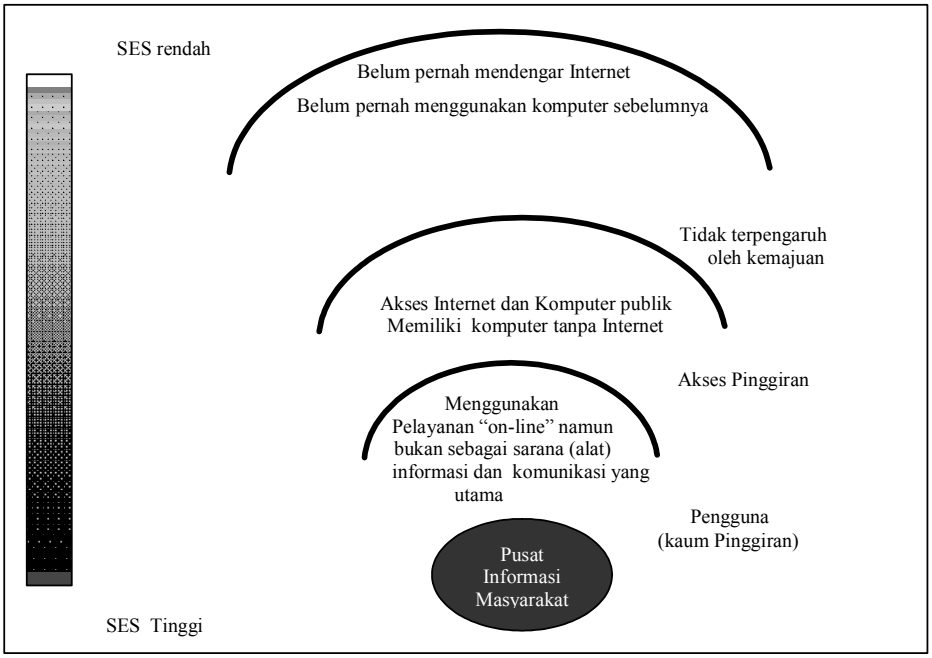
(5) Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

"Cybercrime" di Indonesia

Di antara negara berkembang, Indonesia termasuk negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia tidak memrioritaskan strategi pengembangan dan penguasaan teknologi. Yang terjadi kemudian, transfer teknologi dari negara maju tidak serta merta diikuti dengan penguasaan teknologi oleh negara berkembang seperti Indonesia. Bandingkan saja dengan Malaysia yang telah memproduksi secara massal *software*, per*sonal Computer* (PC), dan ponsel. Sungguh ironis memang, karena menjelang 1980-an Indonesia adalah negara Asia Tenggara pertama yang memiliki satelit komunikasi. Singapura dan Malaysia yang saat itu masih menyewa satelit Palapa dari Indonesia, kini menjadi negara maju berbasis teknologi komunikasi modern.

Meski masih diperdebatkan, dapat dikatakan Indonesia merupakan negara yang memiliki kesenjangan digital yang cukup lebar. Kesenjangan digital dapat diartikan sebagai adanya jurang di antara mereka yang mampu mengakses teknologi komunikasi dan yang tidak mampu (Staubhaar & La Rose, 2000:9). Selain masih senjangnya tingkat pendidikan dan ekonomi di Indonesia, kesempatan

Gambar 1: Model Pusat-Pinggiran Akses Teleteknologi



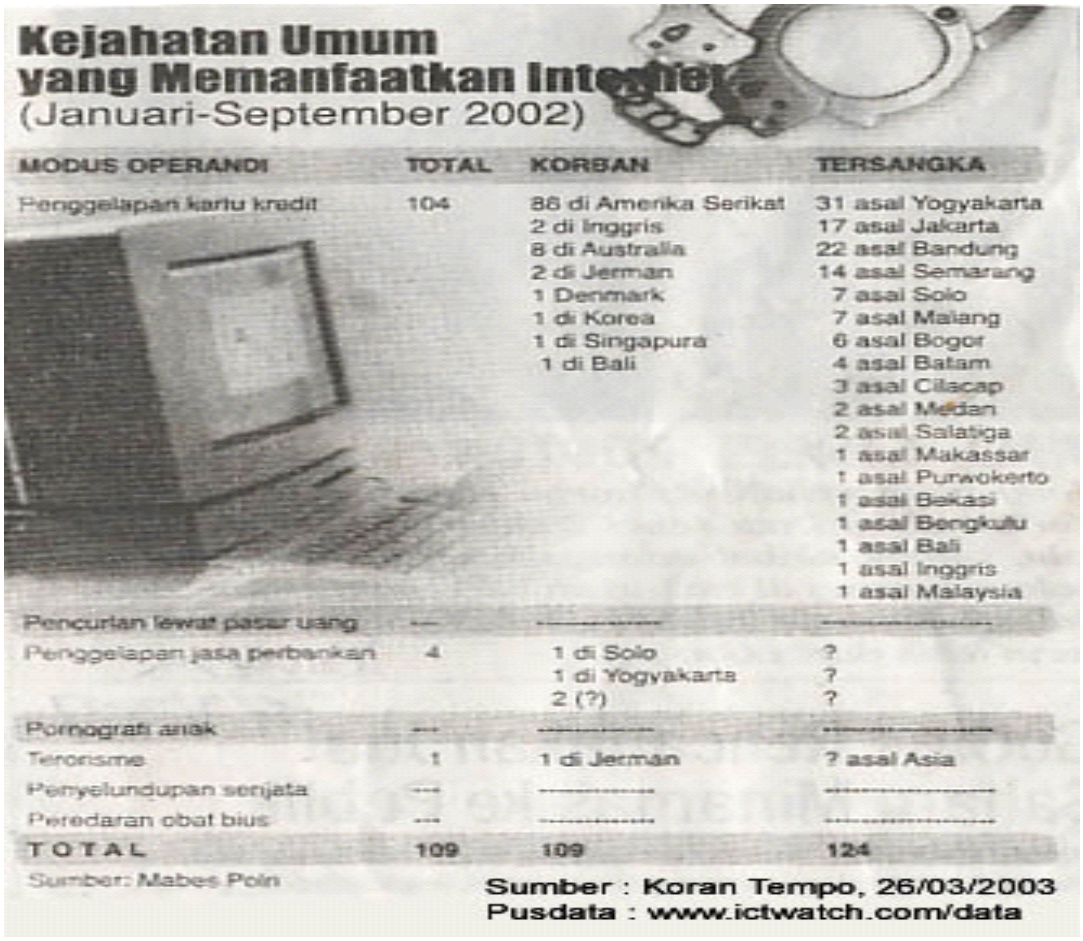
Sumber: Wilhelm (2003:119)

untuk menggunakan teknologi komunikasi di Indonesia belum merata. Ketimpangan, ketidakmilikan informasi dan telekomunikasi dapat dibagi dalam beberapa kategori. Yang paling banyak aksesnya, tentu saja, yang paling dekat dengan pusat informasi masyarakat.

Meskipun terdapat kesenjangan digital, di Indonesia marak sekali kejahatan *cyber*. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para *hacker* hitam. Mereka bisa memperoleh barang apa pun yang diinginkan, mulai dari berlian, radar laut, *corporate software*, *computer server*, Harley Davidson, hingga senjata M-16 (*Warta Ekonomi.com*, 23 Desember 2002) dengan menggunakan kartu kredit milik orang lain. Istilahnya adalah c*arding*. Para *carder* (*hacker* hitam) memesan barang-barang melalui internet untuk dikirimkan ke negara mereka berada. Barang yang dipesan dapat digunakan sendiri, dapat pula dijual dengan harga yang sangat murah. Misalnya, *Notebook* bermerk *Sony* seharga 20 Juta yang dipesan melalui *carding*, dijual seharga 4 Juta rupiah. Untuk yang satu ini, *ClearCommerce*, perusahaan keamanan internet yang berbasis di Texas, Amerika Serikat, memasukkan Indonesia ke dalam daftar negara-negara terburuk untuk kejahatan yang memanfaatkan kecanggihan teknologi komunikasi. Setidaknya, 20 persen transaksi kartu kredit internet yang berasal dari Indonesia merupakan penipuan. Berikut ini adalah data kejahatan yang memanfaatkan internet:

Dari data di bawah (*Koran Tempo*, 26 Maret 2003), Yogyakarta menempati urutan pertama dan Bandung kedua dalam *cybercrime* jenis *carding di* Indonesia. Yang melakukan jenis kejahatan itu adalah kalangan muda, biasanya mahasiswa. Seorang mahasiswa universitas swasta di Bandung pernah memesan 5 buah ponsel *Nokia Communicator* yang ia jual seharga 5 Juta rupiah, padahal saat itu harganya berkisar 10 Juta rupiah.

Gambar 2: Kejahatan Umum yang Memanfaatkan Internet



Kejahatan Umum yang Memanfaatkan Internet
(Januari-September 2002)

MODUS OPERANDI	TOTAL	KORBAN	TERSANGKA
Penggelapan kartu kredit	104	86 di Amerika Serikat 2 di Inggris 8 di Australia 2 di Jerman 1 Denmark 1 di Korea 1 di Singapura 1 di Bali	31 asal Yogyakarta 17 asal Jakarta 22 asal Bandung 14 asal Semarang 7 asal Solo 7 asal Malang 6 asal Bogor 4 asal Batam 3 asal Cilacap 2 asal Medan 2 asal Salatiga 1 asal Makassar 1 asal Purwokerto 1 asal Bekasi 1 asal Bengkulu 1 asal Bali 1 asal Inggris 1 asal Malaysia
Pencurian lewat pasar uang	---	----------	----------
Penggelapan jasa perbankan	4	1 di Solo 1 di Yogyakarta 2 (?)	? ? ?
Pornografi anak	---	----------	----------
Terorisme	1	1 di Jerman	? asal Asia
Penyelundupan senjata	---	----------	----------
Peredaran obat bius	---	----------	----------
TOTAL	109	109	124

Sumber: Mabes Polri

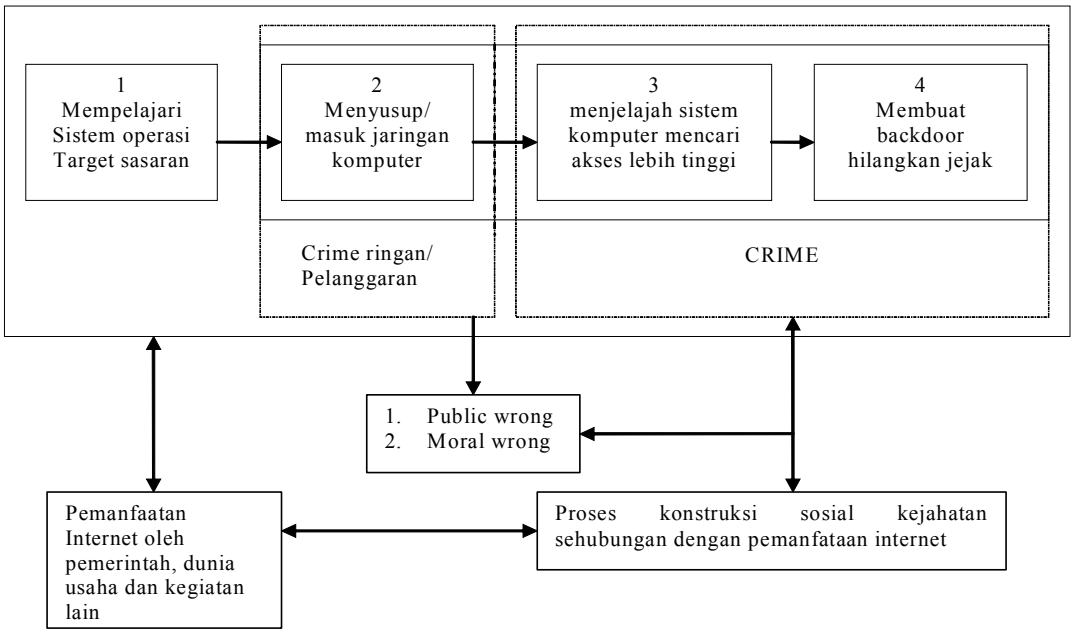
Sumber : Koran Tempo, 26/03/2003
Pusdata : www.ictwatch.com/data

Agar tidak diketahui identitasnya, ia melakukan *carding* di warnet sekitar kampus dan saat mengambil pesanan, agar dimudahkan, ia bekerjasama dan memberi sejumlah uang kepada oknum karyawan biro pengiriman paket terkemuka di Indonesia.

Indonesia tampaknya akan semakin mengukuhkan diri sebagai negara kampiun penipuan kartu kredit di internet Dalam berbagai urusan yang berkonotasi buruk, Indonesia memang seringkali termasuk di dalamnya, mulai dari pendapatan perkapita yang rendah, mutu pendidikan, tingkat korupsi, termasuk *cybercrime* jenis *carding*.

Kejahatan memang tidak dapat diprediksi kejadiannya, tidak mempedulikan tempat dan suasana ketika hendak muncul, tidak pula membanding-bandingkan siapa pelaku dan korbannya, tidak mengenal kasta ataupun status sosial pelaku dan korbannya. Saat muncul, ia dapat menjadi bahan yang menarik untuk dibicarakan, baik di media massa maupun ruang-ruang seminar. Apalagi saat kejahatan itu dipadukan dengan kecanggihan teknologi komunikasi. Tanpa sadar

Gambar 3. Bagan Konstruksi Kejahatan dari "Hacking"



Sumber: Raharjo (2002)

di sekeliling kita terdapat kejahatan yang "*innocent*", seolah tanpa dosa dan begitu halus.

Adapun konstruksi kejahatan *Hacking* dapat dilihat pada gambar 3.

Selain *cybercrime* jenis *carding*, di Indonesia juga sering terjadi kasus *deface*. Tampilan situs di Internet dirusak dan diganti oleh para *hacker* hitam. Berikut ini adalah kasus-kasus yang pernah terjadi (Raharjo, 202:35):

(a) Tahun 1997 ketika masalah Timor-Timur menghangat, situs milik Departemen Luar Negri dan ABRI (TNI, pen) dijebol oleh *craker Porto* (Portugis) yang pro-kemerdekaan. Mereka juga merusak situs-situs bisnis dan pendidikan. Serangan dari *craker* Porto ini mendapat balasan dari *craker* Indonesia. Hal ini dilakukan karena, menurut mereka, *craker* Porto dinilai keterlaluan, serangannya membabi-buta, tidak mempedulikan apakah itu situs milik pemerintah ataupun bukan, situs bisnis maupun situs pendidikan.
(b) Tahun 1998, tampilan depan atau *frontpage* Pusat Dokumentasi Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) diganti dengan gambar wanita telanjang.
(c) Tahun 1998, setelah kerusuhan 13–14 Mei, *craker* yang diduga berasal dari Cina menghantam situs milik pemerintah, yaitu BKKBN. Serangan ini merupakan reaksi atas pemberitaan media mengenai kerusuhan Mei yang menyebabkan etnis Cina di Indonesia menjadi korban pembantaian dan pemerkosaan.
(d) Juni 1999, *homepage* POLRI diganti dengan gambar telanjang, kemudian diganti lagi dengan gambar yang mirip logo PDI-Perjuangan.
(e) Januari 2000, situs yang diserang, antara lain Bursa Efek Jakarta (BEJ), Bank Central Asia dan Indosatnet.

(f) September dan Oktober 2000, Fabian Clone berhasil menjebol web milik Bank Bali, sebelumnya juga berhasil menjebol *web* milik Bank Lippo. Kedua bank itu memberikan layanan *Internet Banking*, kerugian yang diderita lebih besar dibandingkan kerugian yang diderirta BEJ.

(g) Januari 2001, situs milik PT. Ajinomoto Indonesia diserang *craker*. Serangan ini merupakan reaksi atas penggunaan *enzim porcine* (babi) yang digunakan sebagai katalis dalam proses pembuatan bumbu penyedap rasa. Situs Ajinomoto hhtp://www.mjk.ajinomoto.co.id ketika dibuka yang muncul adalah gambar seekor babi yang tengah tersenyum dengan tulisan *Babi, open in December 2K, "Ajinomoto You Lied to Us", "Ajinomoto: HARAM...HARAM...HARAM"*.

(h) Pada 8 Mei 2001, situs Polri mendapat serangan dari Kesatuan Aksi *Hacker* Muslim Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando Jihad.

Bila tidak ditangani dengan baik, ada kemungkinan jumlah kasus berikut korban akan bertambah, baik *cybercrime* dalam bentuk *carding* maupun *deface*, termasuk *cyberporn* meskipun tidak semua publik sepakat bahwa itu adalah suatu kejahatan. Namun, dapat dibayangkan bila orang-orang di sekitar kita, misalnya isteri dan anak kita yang tidak bersalah, tiba-tiba fotonya terpampang di internet dalam keadaan tanpa pakaian dengan teknik rekayasa foto melalui komputer.

Urgensi Penyelesaian "Cybercrime" di Indonesia

Berdasarkan berbagai kasus *cybercrime* yang telah terjadi dan pasti akan bertambah, perlu kiranya dilakukan percepatan dalam menuntaskan kasus *cybercrime*. Untuk menghadapi sekian banyak varian dan modifikasi modus kejahatan di Internet, maka langkah represif dan reaktif yang selama ini dilakukan oleh aparat penegak hukum tidaklah memadai. Aparat tidak siap menghadapinya. Maraknya *cybercrime* menunjukkan ketidakberdayaan pemerintah dalam menyelesaikannya. Oleh karena itu, pemerintah harus meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi, dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*. Aparat kepolisian perlu menanggapi secara serius kejahatan saiber.

Tentunya, harus dibarengi pula dengan serangkaian langkah proaktif dan antisipatif yang dilakukan oleh beragam institusi terkait di Indonesia. Misalnya, asosiasi yang membawahi para *Internet Service Provider* (ISP) dan warnet di Indonesia harus memikirkan langkah yang akan diambil untuk melindungi para konsumen.

Selanjutnya, adalah dengan melakukan kampanye dan edukasi tentang ber-internet yang aman secara komprehensif dan berkala kepada masyarakat umum. Jika hal tersebut tidak segera dilakukan, maka kita harus siap menerima kenyataan bahwa peningkatan penetrasi Internet di Indonesia akan berbanding lurus dengan meningkatnya angka kejahatan Internet secara kuantitatif dan kualitatif. Ujung-ujungnya, hal tersebut justru akan menghancurkan kegiatan usaha/bisnis dan industri internet di Indonesia. Seperti pemblokiran yang dilakukan komunitas internet internasional terhadap pengguna internet dengan nomor *Internet Provider* (IP) Indonesia, sehingga kegiatan bisnis di dunia *cyber* tidak mungkin dilakukan. Itu semua akan menghancurkan kegiatan ekonomi melalui internet.

Tidak kalah pentingnya pula, pemerintah harus bergegas membuat UU *Cyberlaw* untuk menuntaskan kasus *cybercrime*. Perlu dipahami bahwa kegiatan bisnis melalui internet telah mengubah tatanan ekonomi konvesional. Hal itu memunculkan ketidakpastian, karena pihak yang berkomunikasi tidak bertemu secara tatap muka. Untuk memberikan kepastian, perlu dilindungi oleh *cyberlaw*. Meskipun pengguna internet di Indonesia kurang dari 5 % total populasi penduduk (data lainnya menyebutkan hanya 1,9 % atau sekitar 4,38 juta), *cyberlaw* tetap diperlukan sebagai pegangan hukum bagi aparat dalam menuntaskan *cybercrime*. Akan lebih buruk bila tak ada perangkat hukum yang memadai.

Daftar Pustaka

A. Buku

Mahayana, Dimitri. 1999. *Menjemput Masa Depan*, Bandung: PT. Remaja Rosdakarya.

Naisbitt, John, Naisbitt, Nana, & Philips, Douglas. 2001. *High Tech High Touch*. Bandung: Mizan Pustaka.

Piliang, Yasraf Amir. 2001. *Sebuah Dunia yang Menakutkan*. Bandung: Mizan Pustaka.

Raharjo, Agus. 2002. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*. Bandung: Citra Aditya Bakti.

Staubhaar, J. & La Rose, R., *Media Now,* 2000.

Temporal, Paul, K.C. Lee. 2001. *Hi-Tech Hi Touch Branding*. Jakarta: Salemba Empat.

Ustadiyanto, Riyeke. 2001. *Framework e-Commerce*. Yogyakarta: Andi

Wilhelm, Anthony G, *Demokrasi di Era Digital*. 2003. Yogyakarta: Pustaka Pelajar.

B. Sumber lain:

Kompas Cyber Media, 05 Mei 2002.

Republika, 22 Agustus 1999.

komputeraktif, No. 43/18 Desember 2002.

Cybercrime_files\inline_files\SI10.HTM.

Warta Ekonomi.com, 23 Desember 2002.

Terakreditasi Dirjen Dikti SK No. 56/DIKTI/Kep/2005

"Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia

M.E. Fuady

ABSTRACT

It had been long known that technology, as Janus, has two side of coins: the good side, and the bad side. Everybody knows the benefit of technology development. But there aren't much who realize the negative potent of technology. Cybercrime discussed in this article is an example of how crime was developed sophisticatedly by using technological means. Cybercrime, simply defined as criminal acts using cyber and Internet, has faced a new challenge for lawmaker and law enforcement mission. In Indonesia, carding become serious issues to be combated. Another type of cybercrime frequently occur in Indonesia are hacking and deface. Although Internet user in Indonesia is estimated no more than 5% of total population (4.38 million persons), everybody must attended cybercrime issues seriously. The loss of cybercrime reached unspeakable heights and damaged public safety in communication and information flows.

Kata kunci: "cybercrime", realitas virtual, dunia tanpa batas

Internet: Teknologi Pencipta Dunia "Cyber"

Kehadiran teknologi komunikasi modern seperti internet telah membuat pandangan manusia mengenai kehidupan berubah. Paradigma komunikasi manusia dalam menjalani aktivitas ekonomi, bisnis, interaksi sosial, dan politik, menjadi berbeda. Sebelumnya, manusia didominasi oleh aktivitas yang bersifat fisik, *face to face*. Manusia dihalangi oleh berbagai keterbatasan. Dengan internet, ruang, jarak, dan waktu yang membatasi manusia menghilang. Menurut Kenichi Ohmae (Mahayana, 1999:97), itulah dunia tanpa batas (*the borderless world*).

Internet merupakan jaringan dari jutaan komputer yang saling terhubungkan. Dengan internet, setiap orang di seluruh dunia dapat berkomunikasi hanya dengan menekan *keyboard* dan *mouse* di hadapannya. Informasi apa pun yang dibutuhkan telah tersedia. Karena kemudahan yang ditawarkan itulah banyak individu yang menggunakannya. Dibandingkan radio dan televisi, penetrasi internet di kalangan masyarakat, termasuk yang paling cepat. Untuk mencapai pengguna sebanyak 50 juta orang, internet hanya membutuhkan waktu 5 tahun, sementara radio membutuhkan waktu 38 tahun dan televisi 13 tahun (Temporal & Lee, 2002:7). Saat ini, diperkirakan pengguna internet telah mencapai 220 juta orang.

Dengan menggunakan internet, *user* berkesempatan untuk berpetualang, berkelana, berselancar menelusuri *cyberspace*, sebuah dunia komunikasi berbasis komputer (*computer mediated communication*). Realitas yang ditawarkan adalah realitas virtual, kehadirannya tidak dapat ditangkap

atau dipegang tangan, tetapi dikonstruksikan secara sosial oleh orang-orang yang menggeluti teknologi komunikasi dan informasi. Realitas *cyberspace* adalah kenyataan yang melampaui dan artifisial (*hyperreal*). Menurut Piliang (2001), karena rekayasa sedemikian rupa, kenyataan (*real*) ditutupi oleh tanda kenyataan (*sign of real*) sedemikian rupa, sehingga antara tanda dan relitas, antara model dan kenyataan, tidak lagi dapat dibedakan.

Cyberspace menawarkan segala hal yang diperlukan manusia, termasuk kesenangan, keuntungan, dan kemudahan tanpa bersusah payah menggerakkan badan untuk memeroleh sesuatu. Berbagai informasi gratis dari surat kabar dalam dan luar negeri dapat diperoleh tanpa membeli. Menikmati musik tanpa harus membeli kaset. Bagi dosen, berbagai literatur tersaji secara gratis tanpa harus pergi ke tempat berada. Inilah "zona mabuk teknologi" yang dikemukakan Philips dan Naisbitt (2001).

Kehidupan virtual yang disajikan *cyberspace* telah memunculkan bentuk aktivitas baru untuk mencapai kepuasan, seperti *teleshopping*, *teleconference*, *virtual gallery*, *virtual museum*, *e-commerce*, namun juga memunculkan penyimpangan-penyimpangan seperti kejahatan dengan memanfaatkan internet atau *cybercrime*.

"Cybercrime": Bentuk Kejahatan di Dunia Maya

Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime. The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai:"…*any illegal act requiring knowledge of 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*". Hamzah (1989) mengartikan: "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dari beberapa pengertian di atas, Wisnubroto (1999) merumuskan *computer crime* sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas, *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih. Selanjutnya, disebabkan kejahatan itu dilakukan di ruang *cyber* melalui internet, muncul istilah *cybercrime*.

Bagi sebagian besar masyarakat yang terbiasa menggunakan media teknologi komunikasi (telekomunikasi), *cybercrime* bukanlah istilah yang asing terdengar. *Cybercrime* atau kejahatan di ruang maya merupakan sebuah fenomena yang tidak terbantahkan. Tidak terlihat namun nyata. Terdapat berbagai kasus *cybercrime* yang kian hari kian meningkat, terutama di negara-negara yang tidak memiliki kepastian hukum dalam bidang teknologi komunikasi modern (*convergence*).

Teknologi komunikasi yang memiliki kekuatan dahsyat dalam merubah perilaku komunikasi manusia, selain membawa keuntungan berupa kemudahan dalam berkomunikasi, ternyata memiliki "sisi gelap". Teknologi membawa kerugian, salah satunya berupa semakin dipermudahkannya "penjahat" dalam melakukan kejahatannya. Kecanggihan teknologi memungkinkan penjahat *cyber* memangsa korban-korbannya. Meski tidak mau disebut sebagai pelaku kriminal, sebagai akibat dari perbuatannya, mereka tidak ada bedanya dengan seorang penjahat.

Menurut Raharjo (2002:29), sebagai sebuah gejala sosial, kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern). Kejahatan konvensional di dunia nyata muncul dalam dunia maya (*virtual*) dengan wajah kejahatan yang telah diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau *cybercrime* membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, tidak merasakannya sebagai sebuah bentuk kejahatan. Padahal, sudah begitu banyak korban (*victim*) dan

kerugian moril dan materil akibat *cybercrime*. Korbannya dapat berupa *netizen* (penduduk dunia *virtual*/penghuni *cyberspace*) dan masyarakat luas yang awam.

Perusahaan yang bergerak dalam bidang bisnis dan individu tak berdosa, yang tidak memiliki keahlian bahkan pemahaman akan teknologi komunikasi, dapat menjadi korban. Tidak perlu jauh-jauh, kita semua masih ingat dengan kasus mahasiswa dan artis "bugil" yang beredar di internet. Sedikit sekali di antara mereka yang memahami teknologi komunikasi, tetapi mereka telah menjadi korban. Sebut saja artis dengan inisial YS, KD, KF, CK, dan masih banyak lagi. Itu salah satu contoh kecil korban dari *cybercrime*. Meski memang ada publik yang tidak menyepakati *cyberporn* sebagai *cybercrime*. Tetapi, kita telah melihat adanya korban akibat perbuatan pelaku *cybercrime*. Sebagai catatan penting, menurut Menteri Negara Komunikasi dan Informasi, sekitar 50 persen kalangan muda yang menggunakan internet lebih suka untuk mengunjungi situs porno (*Kompas Cyber Media*, 05 Mei 2002).

Untuk memahami *cybercrime*, perlu kiranya dipahami terlebih dahulu apa yang disebut dengan *hacker*, *cracker* dan beberapa lainnya. Karena, seperti halnya kehidupan nyata, ada di antara mereka yang "hitam" dan "putih", ada yang berlaku seperti pahlawan dan penjahat.

(1) *Hacker*

Hacker secara harfiah berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup melalui komputer ke dalam jaringan komputer (*Republika*, 22 Agustus 1999). Menurut Ustadiyanto (2001:304), ada definisi yang relevan, yakni *hacker* adalah orang-orang yang ahli dalam bidangnya. Bila komputer, maka dia pandai menggunakannya. Ia sangat menguasai komputer. *Hacker* adalah orang-orang yang gemar mempelajari seluk-beluk sistem komputer dan bereksperimen dengannya. Mereka pandai untuk menyusup ke dalam jaringan komunikasi suatu institusi di dunia maya. *Hacker* menjunjung tinggi etika atau norma yang berlaku di dunia maya. Mereka anti penyensoran, anti penipuan, dan pemaksaan kehendak pada orang lain. Mereka memegang prinsip bahwa meng-*hack* untuk tujuan meningkatkan keamanan jaringan internet. Misalnya, bila ada sebuah perusahaan perbankan mengatakan bahwa jaringan sistem komunikasi mereka sudah sangat canggih dan mustahil dibobol, tidak dapat ditembus oleh siapa pun, maka *hacker* tertantang untuk mencoba dan setelah berhasil mereka memperingatkan betapa lemahnya sistem informasi perusahaan terrsebut. Oleh karena itu, tidak sedikit dari mereka yang akhirnya direkrut perusahaan untuk mengamankan sistem informasi dan komunikasi di dunia maya.

(2) *Cracker*

Di dunia *cyber*, ada pula *hacker* yang memiki sisi gelap. Mereka disebut *cracker*. Para *cracker* ini secara ilegal melakukan penyusupan dan perusakan terhadap situs, *website,* dan sistem keamanan jaringan internet untuk memperoleh kesenangan dan keuntungan. Mereka bangga dan sombong atas keberhasilan mereka merusak situs sebuah perusahaan. Serangannya sangat luar biasa. Kementerian Petahanan Amerika Serikat di Pentagon mencatat serangan 100 *cracker* dalam satu hari (*Republika*, 6 Januari 2000).

(3) *Carder*

Carder adalah orang yang melakukan *cracking*, yakni pembobolan terhadap kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk kepentingan pribadi. Biasanya yang menjadi korbannya adalah mereka yang memiliki kartu kredit dalam jumlah besar. Menurut hasil riset, pada tahun 2002, Indonesia menempati urutan kedua setelah Ukraina dalam kejahatan *carding*.

(4) *Deface*

Deface adalah tindakan menyusup ke suatu situs, lalu mengubah tampilan halaman dari situs dengan tujuan tertentu. Indonesia pernah diserang para *deface* yang mengubah situs TNI. Tampilan gambar Burung Garuda Pancasila diganti dengan lambang palu arit. *Hompage* Polri diganti tampilannya dengan

gambar wanita telanjang.

(5) *Phreaker*
*Yaitu ses*eorang yang melakukan *cracking* terhadap jaringan telepon, sehingga dapat menelepon secara gratis ke daerah manapun yang dituju (*Komputeraktif*, No. 43/18 Desember 2002). Di Indonesia, kasus semacam ini pernah terjadi pada wartel–wartel.

Para pelaku *hacking* biasanya bukan dari kalangan lapisan bawah, pada umumnya mereka adalah kaum terpelajar, setidak-tidaknya mengenyam pendidikan formal sampai tingkat tertentu dan dapat menggunakan atau mengoperasikan komputer. Para *craker* adalah orang yang berpendidikan, tidak buta teknologi, secara ekonomis mampu dan tidak termasuk dalam masyarakat lapisan bawah. Kejahatan ini dapat dikategorikan kepada *white collar crime* (kejahatan kerah putih). Jo Ann L. Miller, mengkategorikan pelakunya menjadi 4 (empat).

(a) *Organizational occupational crime*
Pelakunya adalah para eksekutif. Mereka melakukan perbuatan ilegal atau merugikan orang lain melalui jaringan internet demi kepentingan atau keuntungan korporasi.

(b) *Government occupational crime*
Pelakunya adalah pejabat atau birokrat yang melakukan perbuatan ilegal melalui internet atas persetujuan atau perintah negara atau pemerintah, meski dalam banyak kasus, bila terungkap hal itu akan disangkal.

(c) *Professional occupational crime*
Berbagai profesi yang melakukan kejahatan secara sengaja (*malpractice*).

(d) *Individual occupational crime*
Perilaku menyimpang yang dilakukan oleh para pengusaha, pemilik modal atau orang-orang independen lainnya, walau mungkin tidak tinggi tingkat sosial ekonominya. Dalam bidang kerjanya kalangan ini memilih jalan yang menyimpang yang melanggar hukum atau merugikan orang lain.

Karakteristik "Cybercrime"

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain (CYBERCRIME_files\ inline_files\ SI10.HTM):

(1) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/ wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.

(2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.

(3) Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional

(4) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya

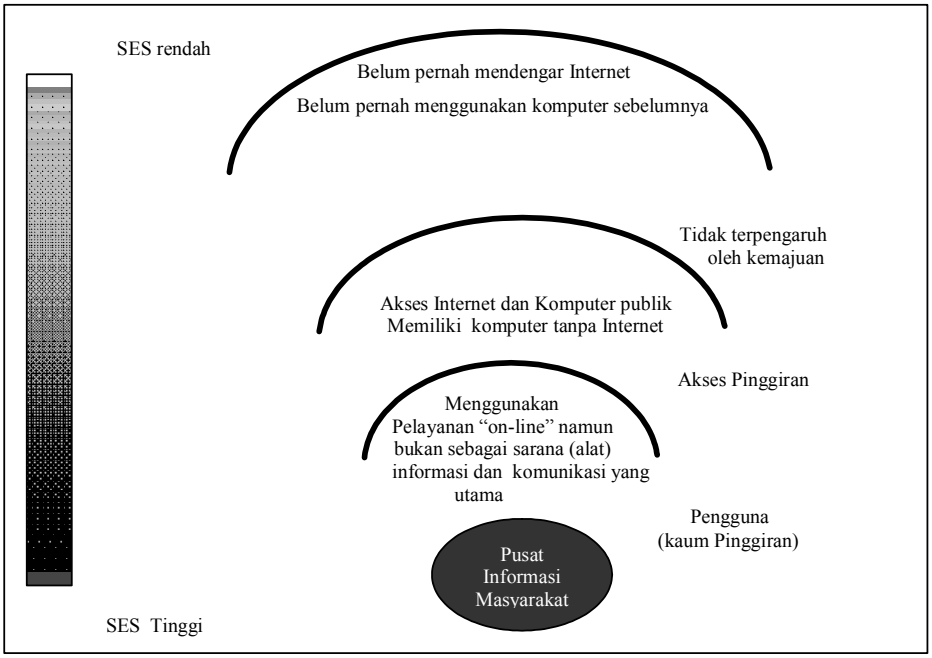
(5) Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

"Cybercrime" di Indonesia

Di antara negara berkembang, Indonesia termasuk negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia tidak memrioritaskan strategi pengembangan dan penguasaan teknologi. Yang terjadi kemudian, transfer teknologi dari negara maju tidak serta merta diikuti dengan penguasaan teknologi oleh negara berkembang seperti Indonesia. Bandingkan saja dengan Malaysia yang telah memproduksi secara massal *software*, per*sonal Computer* (PC), dan ponsel. Sungguh ironis memang, karena menjelang 1980-an Indonesia adalah negara Asia Tenggara pertama yang memiliki satelit komunikasi. Singapura dan Malaysia yang saat itu masih menyewa satelit Palapa dari Indonesia, kini menjadi negara maju berbasis teknologi komunikasi modern.

Meski masih diperdebatkan, dapat dikatakan Indonesia merupakan negara yang memiliki kesenjangan digital yang cukup lebar. Kesenjangan digital dapat diartikan sebagai adanya jurang di antara mereka yang mampu mengakses teknologi komunikasi dan yang tidak mampu (Staubhaar & La Rose, 2000:9). Selain masih senjangnya tingkat pendidikan dan ekonomi di Indonesia, kesempatan

Gambar 1: Model Pusat-Pinggiran Akses Teleteknologi



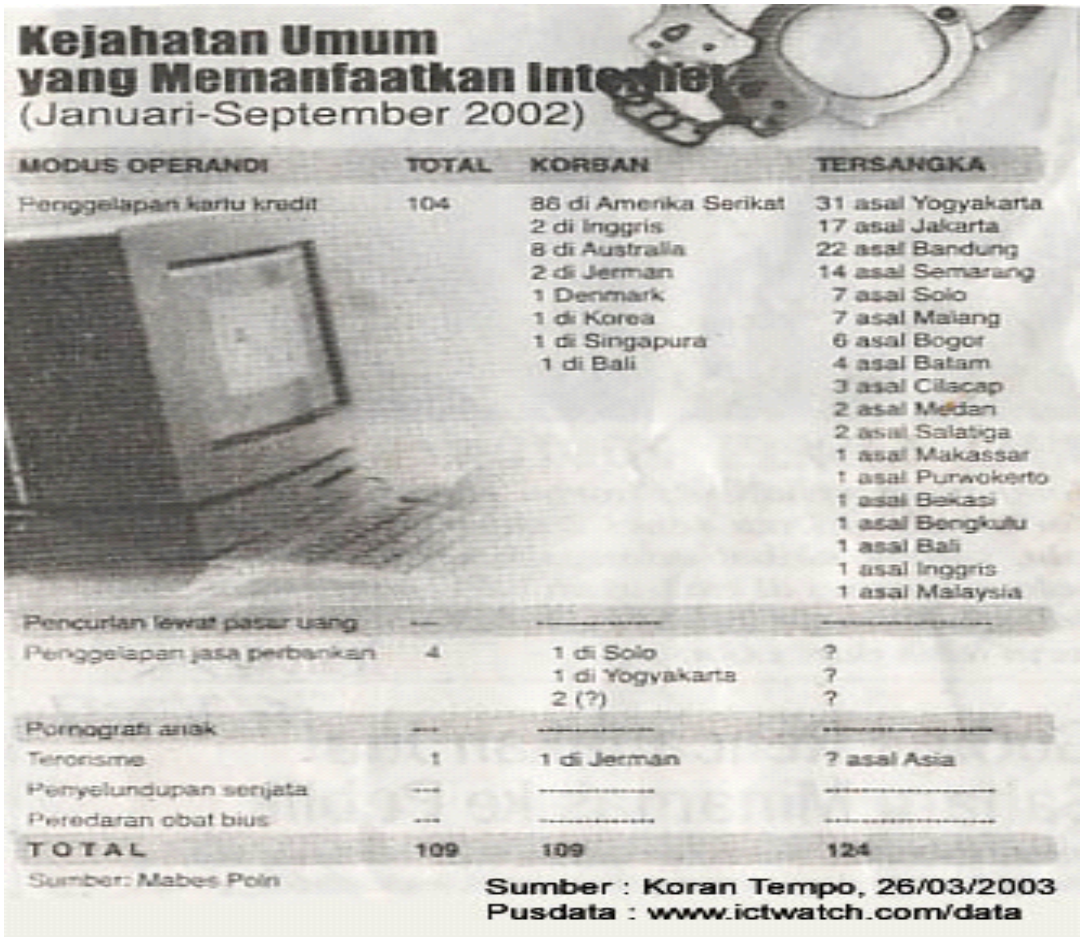
Sumber: Wilhelm (2003:119)

untuk menggunakan teknologi komunikasi di Indonesia belum merata. Ketimpangan, ketidakmilikan informasi dan telekomunikasi dapat dibagi dalam beberapa kategori. Yang paling banyak aksesnya, tentu saja, yang paling dekat dengan pusat informasi masyarakat.

Meskipun terdapat kesenjangan digital, di Indonesia marak sekali kejahatan *cyber*. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para *hacker* hitam. Mereka bisa memperoleh barang apa pun yang diinginkan, mulai dari berlian, radar laut, *corporate software*, *computer server*, Harley Davidson, hingga senjata M-16 (*Warta Ekonomi.com*, 23 Desember 2002) dengan menggunakan kartu kredit milik orang lain. Istilahnya adalah c*arding*. Para *carder* (*hacker* hitam) memesan barang-barang melalui internet untuk dikirimkan ke negara mereka berada. Barang yang dipesan dapat digunakan sendiri, dapat pula dijual dengan harga yang sangat murah. Misalnya, *Notebook* bermerk *Sony* seharga 20 Juta yang dipesan melalui *carding*, dijual seharga 4 Juta rupiah. Untuk yang satu ini, *ClearCommerce*, perusahaan keamanan internet yang berbasis di Texas, Amerika Serikat, memasukkan Indonesia ke dalam daftar negara-negara terburuk untuk kejahatan yang memanfaatkan kecanggihan teknologi komunikasi. Setidaknya, 20 persen transaksi kartu kredit internet yang berasal dari Indonesia merupakan penipuan. Berikut ini adalah data kejahatan yang memanfaatkan internet:

Dari data di bawah (*Koran Tempo*, 26 Maret 2003), Yogyakarta menempati urutan pertama dan Bandung kedua dalam *cybercrime* jenis *carding di* Indonesia. Yang melakukan jenis kejahatan itu adalah kalangan muda, biasanya mahasiswa. Seorang mahasiswa universitas swasta di Bandung pernah memesan 5 buah ponsel *Nokia Communicator* yang ia jual seharga 5 Juta rupiah, padahal saat itu harganya berkisar 10 Juta rupiah.

Gambar 2: Kejahatan Umum yang Memanfaatkan Internet



Kejahatan Umum yang Memanfaatkan Internet
(Januari-September 2002)

MODUS OPERANDI	TOTAL	KORBAN	TERSANGKA
Penggelapan kartu kredit	104	86 di Amerika Serikat 2 di Inggris 8 di Australia 2 di Jerman 1 Denmark 1 di Korea 1 di Singapura 1 di Bali	31 asal Yogyakarta 17 asal Jakarta 22 asal Bandung 14 asal Semarang 7 asal Solo 7 asal Malang 6 asal Bogor 4 asal Batam 3 asal Cilacap 2 asal Medan 2 asal Salatiga 1 asal Makassar 1 asal Purwokerto 1 asal Bekasi 1 asal Bengkulu 1 asal Bali 1 asal Inggris 1 asal Malaysia
Pencurian lewat pasar uang	---	----------	----------
Penggelapan jasa perbankan	4	1 di Solo 1 di Yogyakarta 2 (?)	? ? ?
Pornografi anak	---	----------	----------
Terorisme	1	1 di Jerman	? asal Asia
Penyelundupan senjata	---	----------	----------
Peredaran obat bius	---	----------	----------
TOTAL	109	109	124

Sumber: Mabes Polri

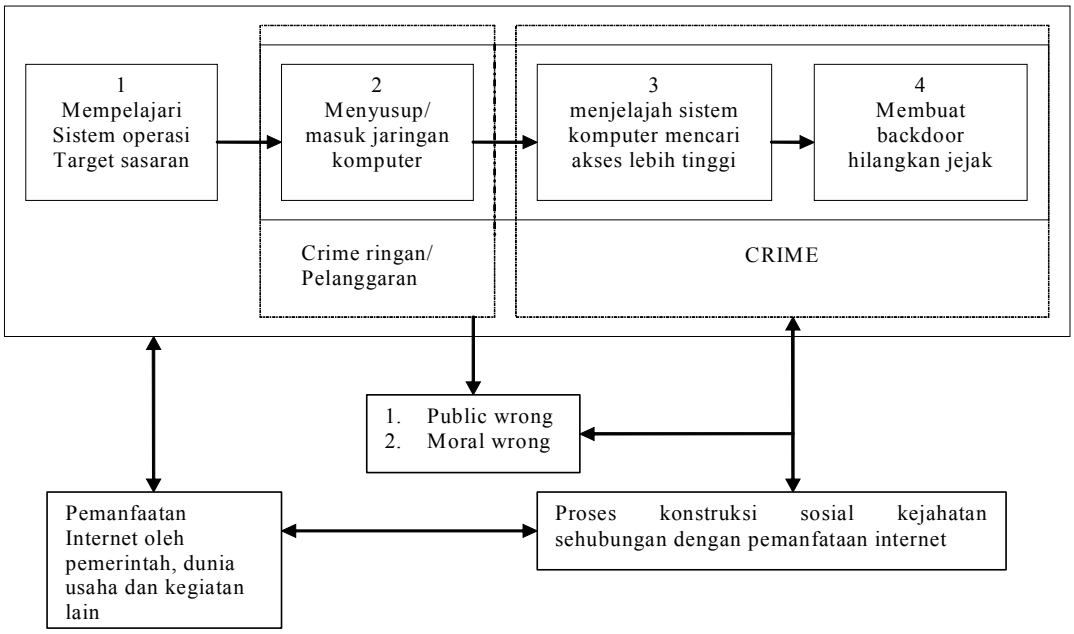
Sumber : Koran Tempo, 26/03/2003
Pusdata : www.ictwatch.com/data

Agar tidak diketahui identitasnya, ia melakukan *carding* di warnet sekitar kampus dan saat mengambil pesanan, agar dimudahkan, ia bekerjasama dan memberi sejumlah uang kepada oknum karyawan biro pengiriman paket terkemuka di Indonesia.

Indonesia tampaknya akan semakin mengukuhkan diri sebagai negara kampiun penipuan kartu kredit di internet Dalam berbagai urusan yang berkonotasi buruk, Indonesia memang seringkali termasuk di dalamnya, mulai dari pendapatan perkapita yang rendah, mutu pendidikan, tingkat korupsi, termasuk *cybercrime* jenis *carding*.

Kejahatan memang tidak dapat diprediksi kejadiannya, tidak mempedulikan tempat dan suasana ketika hendak muncul, tidak pula membanding-bandingkan siapa pelaku dan korbannya, tidak mengenal kasta ataupun status sosial pelaku dan korbannya. Saat muncul, ia dapat menjadi bahan yang menarik untuk dibicarakan, baik di media massa maupun ruang-ruang seminar. Apalagi saat kejahatan itu dipadukan dengan kecanggihan teknologi komunikasi. Tanpa sadar

Gambar 3. Bagan Konstruksi Kejahatan dari "Hacking"



Sumber: Raharjo (2002)

di sekeliling kita terdapat kejahatan yang "*innocent*", seolah tanpa dosa dan begitu halus.

Adapun konstruksi kejahatan *Hacking* dapat dilihat pada gambar 3.

Selain *cybercrime* jenis *carding*, di Indonesia juga sering terjadi kasus *deface*. Tampilan situs di Internet dirusak dan diganti oleh para *hacker* hitam. Berikut ini adalah kasus-kasus yang pernah terjadi (Raharjo, 202:35):

(a) Tahun 1997 ketika masalah Timor-Timur menghangat, situs milik Departemen Luar Negri dan ABRI (TNI, pen) dijebol oleh *craker Porto* (Portugis) yang pro-kemerdekaan. Mereka juga merusak situs-situs bisnis dan pendidikan. Serangan dari *craker* Porto ini mendapat balasan dari *craker* Indonesia. Hal ini dilakukan karena, menurut mereka, *craker* Porto dinilai keterlaluan, serangannya membabi-buta, tidak mempedulikan apakah itu situs milik pemerintah ataupun bukan, situs bisnis maupun situs pendidikan.
(b) Tahun 1998, tampilan depan atau *frontpage* Pusat Dokumentasi Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) diganti dengan gambar wanita telanjang.
(c) Tahun 1998, setelah kerusuhan 13–14 Mei, *craker* yang diduga berasal dari Cina menghantam situs milik pemerintah, yaitu BKKBN. Serangan ini merupakan reaksi atas pemberitaan media mengenai kerusuhan Mei yang menyebabkan etnis Cina di Indonesia menjadi korban pembantaian dan pemerkosaan.
(d) Juni 1999, *homepage* POLRI diganti dengan gambar telanjang, kemudian diganti lagi dengan gambar yang mirip logo PDI-Perjuangan.
(e) Januari 2000, situs yang diserang, antara lain Bursa Efek Jakarta (BEJ), Bank Central Asia dan Indosatnet.

(f) September dan Oktober 2000, Fabian Clone berhasil menjebol web milik Bank Bali, sebelumnya juga berhasil menjebol *web* milik Bank Lippo. Kedua bank itu memberikan layanan *Internet Banking*, kerugian yang diderita lebih besar dibandingkan kerugian yang diderirta BEJ.

(g) Januari 2001, situs milik PT. Ajinomoto Indonesia diserang *craker*. Serangan ini merupakan reaksi atas penggunaan *enzim porcine* (babi) yang digunakan sebagai katalis dalam proses pembuatan bumbu penyedap rasa. Situs Ajinomoto hhtp://www.mjk.ajinomoto.co.id ketika dibuka yang muncul adalah gambar seekor babi yang tengah tersenyum dengan tulisan *Babi, open in December 2K, "Ajinomoto You Lied to Us", "Ajinomoto: HARAM...HARAM...HARAM"*.

(h) Pada 8 Mei 2001, situs Polri mendapat serangan dari Kesatuan Aksi *Hacker* Muslim Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando Jihad.

Bila tidak ditangani dengan baik, ada kemungkinan jumlah kasus berikut korban akan bertambah, baik *cybercrime* dalam bentuk *carding* maupun *deface*, termasuk *cyberporn* meskipun tidak semua publik sepakat bahwa itu adalah suatu kejahatan. Namun, dapat dibayangkan bila orang-orang di sekitar kita, misalnya isteri dan anak kita yang tidak bersalah, tiba-tiba fotonya terpampang di internet dalam keadaan tanpa pakaian dengan teknik rekayasa foto melalui komputer.

Urgensi Penyelesaian "Cybercrime" di Indonesia

Berdasarkan berbagai kasus *cybercrime* yang telah terjadi dan pasti akan bertambah, perlu kiranya dilakukan percepatan dalam menuntaskan kasus *cybercrime*. Untuk menghadapi sekian banyak varian dan modifikasi modus kejahatan di Internet, maka langkah represif dan reaktif yang selama ini dilakukan oleh aparat penegak hukum tidaklah memadai. Aparat tidak siap menghadapinya. Maraknya *cybercrime* menunjukkan ketidakberdayaan pemerintah dalam menyelesaikannya. Oleh karena itu, pemerintah harus meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi, dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*. Aparat kepolisian perlu menanggapi secara serius kejahatan saiber.

Tentunya, harus dibarengi pula dengan serangkaian langkah proaktif dan antisipatif yang dilakukan oleh beragam institusi terkait di Indonesia. Misalnya, asosiasi yang membawahi para *Internet Service Provider* (ISP) dan warnet di Indonesia harus memikirkan langkah yang akan diambil untuk melindungi para konsumen.

Selanjutnya, adalah dengan melakukan kampanye dan edukasi tentang ber-internet yang aman secara komprehensif dan berkala kepada masyarakat umum. Jika hal tersebut tidak segera dilakukan, maka kita harus siap menerima kenyataan bahwa peningkatan penetrasi Internet di Indonesia akan berbanding lurus dengan meningkatnya angka kejahatan Internet secara kuantitatif dan kualitatif. Ujung-ujungnya, hal tersebut justru akan menghancurkan kegiatan usaha/bisnis dan industri internet di Indonesia. Seperti pemblokiran yang dilakukan komunitas internet internasional terhadap pengguna internet dengan nomor *Internet Provider* (IP) Indonesia, sehingga kegiatan bisnis di dunia *cyber* tidak mungkin dilakukan. Itu semua akan menghancurkan kegiatan ekonomi melalui internet.

Tidak kalah pentingnya pula, pemerintah harus bergegas membuat UU *Cyberlaw* untuk menuntaskan kasus *cybercrime*. Perlu dipahami bahwa kegiatan bisnis melalui internet telah mengubah tatanan ekonomi konvesional. Hal itu memunculkan ketidakpastian, karena pihak yang berkomunikasi tidak bertemu secara tatap muka. Untuk memberikan kepastian, perlu dilindungi oleh *cyberlaw*. Meskipun pengguna internet di Indonesia kurang dari 5 % total populasi penduduk (data lainnya menyebutkan hanya 1,9 % atau sekitar 4,38 juta), *cyberlaw* tetap diperlukan sebagai pegangan hukum bagi aparat dalam menuntaskan *cybercrime*. Akan lebih buruk bila tak ada perangkat hukum yang memadai.

Daftar Pustaka

A. Buku

Mahayana, Dimitri. 1999. *Menjemput Masa Depan*, Bandung: PT. Remaja Rosdakarya.

Naisbitt, John, Naisbitt, Nana, & Philips, Douglas. 2001. *High Tech High Touch*. Bandung: Mizan Pustaka.

Piliang, Yasraf Amir. 2001. *Sebuah Dunia yang Menakutkan*. Bandung: Mizan Pustaka.

Raharjo, Agus. 2002. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*. Bandung: Citra Aditya Bakti.

Staubhaar, J. & La Rose, R., *Media Now,* 2000.

Temporal, Paul, K.C. Lee. 2001. *Hi-Tech Hi Touch Branding*. Jakarta: Salemba Empat.

Ustadiyanto, Riyeke. 2001. *Framework e-Commerce*. Yogyakarta: Andi

Wilhelm, Anthony G, *Demokrasi di Era Digital*. 2003. Yogyakarta: Pustaka Pelajar.

B. Sumber lain:

Kompas Cyber Media, 05 Mei 2002.

Republika, 22 Agustus 1999.

komputeraktif, No. 43/18 Desember 2002.

Cybercrime_files\inline_files\SI10.HTM.

Warta Ekonomi.com, 23 Desember 2002.

Terakreditasi Dirjen Dikti SK No. 56/DIKTI/Kep/2005

"Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia

M.E. Fuady

ABSTRACT

It had been long known that technology, as Janus, has two side of coins: the good side, and the bad side. Everybody knows the benefit of technology development. But there aren't much who realize the negative potent of technology. Cybercrime discussed in this article is an example of how crime was developed sophisticatedly by using technological means. Cybercrime, simply defined as criminal acts using cyber and Internet, has faced a new challenge for lawmaker and law enforcement mission. In Indonesia, carding become serious issues to be combated. Another type of cybercrime frequently occur in Indonesia are hacking and deface. Although Internet user in Indonesia is estimated no more than 5% of total population (4.38 million persons), everybody must attended cybercrime issues seriously. The loss of cybercrime reached unspeakable heights and damaged public safety in communication and information flows.

Kata kunci: "cybercrime", realitas virtual, dunia tanpa batas

Internet: Teknologi Pencipta Dunia "Cyber"

Kehadiran teknologi komunikasi modern seperti internet telah membuat pandangan manusia mengenai kehidupan berubah. Paradigma komunikasi manusia dalam menjalani aktivitas ekonomi, bisnis, interaksi sosial, dan politik, menjadi berbeda. Sebelumnya, manusia didominasi oleh aktivitas yang bersifat fisik, *face to face*. Manusia dihalangi oleh berbagai keterbatasan. Dengan internet, ruang, jarak, dan waktu yang membatasi manusia menghilang. Menurut Kenichi Ohmae (Mahayana, 1999:97), itulah dunia tanpa batas (*the borderless world*).

Internet merupakan jaringan dari jutaan komputer yang saling terhubungkan. Dengan internet, setiap orang di seluruh dunia dapat berkomunikasi hanya dengan menekan *keyboard* dan *mouse* di hadapannya. Informasi apa pun yang dibutuhkan telah tersedia. Karena kemudahan yang ditawarkan itulah banyak individu yang menggunakannya. Dibandingkan radio dan televisi, penetrasi internet di kalangan masyarakat, termasuk yang paling cepat. Untuk mencapai pengguna sebanyak 50 juta orang, internet hanya membutuhkan waktu 5 tahun, sementara radio membutuhkan waktu 38 tahun dan televisi 13 tahun (Temporal & Lee, 2002:7). Saat ini, diperkirakan pengguna internet telah mencapai 220 juta orang.

Dengan menggunakan internet, *user* berkesempatan untuk berpetualang, berkelana, berselancar menelusuri *cyberspace*, sebuah dunia komunikasi berbasis komputer (*computer mediated communication*). Realitas yang ditawarkan adalah realitas virtual, kehadirannya tidak dapat ditangkap

atau dipegang tangan, tetapi dikonstruksikan secara sosial oleh orang-orang yang menggeluti teknologi komunikasi dan informasi. Realitas *cyberspace* adalah kenyataan yang melampaui dan artifisial (*hyperreal*). Menurut Piliang (2001), karena rekayasa sedemikian rupa, kenyataan (*real*) ditutupi oleh tanda kenyataan (*sign of real*) sedemikian rupa, sehingga antara tanda dan relitas, antara model dan kenyataan, tidak lagi dapat dibedakan.

Cyberspace menawarkan segala hal yang diperlukan manusia, termasuk kesenangan, keuntungan, dan kemudahan tanpa bersusah payah menggerakkan badan untuk memeroleh sesuatu. Berbagai informasi gratis dari surat kabar dalam dan luar negeri dapat diperoleh tanpa membeli. Menikmati musik tanpa harus membeli kaset. Bagi dosen, berbagai literatur tersaji secara gratis tanpa harus pergi ke tempat berada. Inilah "zona mabuk teknologi" yang dikemukakan Philips dan Naisbitt (2001).

Kehidupan virtual yang disajikan *cyberspace* telah memunculkan bentuk aktivitas baru untuk mencapai kepuasan, seperti *teleshopping*, *teleconference*, *virtual gallery*, *virtual museum*, *e-commerce*, namun juga memunculkan penyimpangan-penyimpangan seperti kejahatan dengan memanfaatkan internet atau *cybercrime*.

"Cybercrime": Bentuk Kejahatan di Dunia Maya

Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime. The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai:"…*any illegal act requiring knowledge of 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*". Hamzah (1989) mengartikan: "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dari beberapa pengertian di atas, Wisnubroto (1999) merumuskan *computer crime* sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas, *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih. Selanjutnya, disebabkan kejahatan itu dilakukan di ruang *cyber* melalui internet, muncul istilah *cybercrime*.

Bagi sebagian besar masyarakat yang terbiasa menggunakan media teknologi komunikasi (telekomunikasi), *cybercrime* bukanlah istilah yang asing terdengar. *Cybercrime* atau kejahatan di ruang maya merupakan sebuah fenomena yang tidak terbantahkan. Tidak terlihat namun nyata. Terdapat berbagai kasus *cybercrime* yang kian hari kian meningkat, terutama di negara-negara yang tidak memiliki kepastian hukum dalam bidang teknologi komunikasi modern (*convergence*).

Teknologi komunikasi yang memiliki kekuatan dahsyat dalam merubah perilaku komunikasi manusia, selain membawa keuntungan berupa kemudahan dalam berkomunikasi, ternyata memiliki "sisi gelap". Teknologi membawa kerugian, salah satunya berupa semakin dipermudahkannya "penjahat" dalam melakukan kejahatannya. Kecanggihan teknologi memungkinkan penjahat *cyber* memangsa korban-korbannya. Meski tidak mau disebut sebagai pelaku kriminal, sebagai akibat dari perbuatannya, mereka tidak ada bedanya dengan seorang penjahat.

Menurut Raharjo (2002:29), sebagai sebuah gejala sosial, kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern). Kejahatan konvensional di dunia nyata muncul dalam dunia maya (*virtual*) dengan wajah kejahatan yang telah diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau *cybercrime* membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, tidak merasakannya sebagai sebuah bentuk kejahatan. Padahal, sudah begitu banyak korban (*victim*) dan

kerugian moril dan materil akibat *cybercrime*. Korbannya dapat berupa *netizen* (penduduk dunia *virtual*/penghuni *cyberspace*) dan masyarakat luas yang awam.

Perusahaan yang bergerak dalam bidang bisnis dan individu tak berdosa, yang tidak memiliki keahlian bahkan pemahaman akan teknologi komunikasi, dapat menjadi korban. Tidak perlu jauh-jauh, kita semua masih ingat dengan kasus mahasiswa dan artis "bugil" yang beredar di internet. Sedikit sekali di antara mereka yang memahami teknologi komunikasi, tetapi mereka telah menjadi korban. Sebut saja artis dengan inisial YS, KD, KF, CK, dan masih banyak lagi. Itu salah satu contoh kecil korban dari *cybercrime*. Meski memang ada publik yang tidak menyepakati *cyberporn* sebagai *cybercrime*. Tetapi, kita telah melihat adanya korban akibat perbuatan pelaku *cybercrime*. Sebagai catatan penting, menurut Menteri Negara Komunikasi dan Informasi, sekitar 50 persen kalangan muda yang menggunakan internet lebih suka untuk mengunjungi situs porno (*Kompas Cyber Media*, 05 Mei 2002).

Untuk memahami *cybercrime*, perlu kiranya dipahami terlebih dahulu apa yang disebut dengan *hacker*, *cracker* dan beberapa lainnya. Karena, seperti halnya kehidupan nyata, ada di antara mereka yang "hitam" dan "putih", ada yang berlaku seperti pahlawan dan penjahat.

(1) *Hacker*

Hacker secara harfiah berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup melalui komputer ke dalam jaringan komputer (*Republika*, 22 Agustus 1999). Menurut Ustadiyanto (2001:304), ada definisi yang relevan, yakni *hacker* adalah orang-orang yang ahli dalam bidangnya. Bila komputer, maka dia pandai menggunakannya. Ia sangat menguasai komputer. *Hacker* adalah orang-orang yang gemar mempelajari seluk-beluk sistem komputer dan bereksperimen dengannya. Mereka pandai untuk menyusup ke dalam jaringan komunikasi suatu institusi di dunia maya. *Hacker* menjunjung tinggi etika atau norma yang berlaku di dunia maya. Mereka anti penyensoran, anti penipuan, dan pemaksaan kehendak pada orang lain. Mereka memegang prinsip bahwa meng-*hack* untuk tujuan meningkatkan keamanan jaringan internet. Misalnya, bila ada sebuah perusahaan perbankan mengatakan bahwa jaringan sistem komunikasi mereka sudah sangat canggih dan mustahil dibobol, tidak dapat ditembus oleh siapa pun, maka *hacker* tertantang untuk mencoba dan setelah berhasil mereka memperingatkan betapa lemahnya sistem informasi perusahaan terrsebut. Oleh karena itu, tidak sedikit dari mereka yang akhirnya direkrut perusahaan untuk mengamankan sistem informasi dan komunikasi di dunia maya.

(2) *Cracker*

Di dunia *cyber*, ada pula *hacker* yang memiki sisi gelap. Mereka disebut *cracker*. Para *cracker* ini secara ilegal melakukan penyusupan dan perusakan terhadap situs, *website,* dan sistem keamanan jaringan internet untuk memperoleh kesenangan dan keuntungan. Mereka bangga dan sombong atas keberhasilan mereka merusak situs sebuah perusahaan. Serangannya sangat luar biasa. Kementerian Petahanan Amerika Serikat di Pentagon mencatat serangan 100 *cracker* dalam satu hari (*Republika*, 6 Januari 2000).

(3) *Carder*

Carder adalah orang yang melakukan *cracking*, yakni pembobolan terhadap kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk kepentingan pribadi. Biasanya yang menjadi korbannya adalah mereka yang memiliki kartu kredit dalam jumlah besar. Menurut hasil riset, pada tahun 2002, Indonesia menempati urutan kedua setelah Ukraina dalam kejahatan *carding*.

(4) *Deface*

Deface adalah tindakan menyusup ke suatu situs, lalu mengubah tampilan halaman dari situs dengan tujuan tertentu. Indonesia pernah diserang para *deface* yang mengubah situs TNI. Tampilan gambar Burung Garuda Pancasila diganti dengan lambang palu arit. *Hompage* Polri diganti tampilannya dengan

gambar wanita telanjang.

(5) *Phreaker*
*Yaitu ses*eorang yang melakukan *cracking* terhadap jaringan telepon, sehingga dapat menelepon secara gratis ke daerah manapun yang dituju (*Komputeraktif*, No. 43/18 Desember 2002). Di Indonesia, kasus semacam ini pernah terjadi pada wartel–wartel.

Para pelaku *hacking* biasanya bukan dari kalangan lapisan bawah, pada umumnya mereka adalah kaum terpelajar, setidak-tidaknya mengenyam pendidikan formal sampai tingkat tertentu dan dapat menggunakan atau mengoperasikan komputer. Para *craker* adalah orang yang berpendidikan, tidak buta teknologi, secara ekonomis mampu dan tidak termasuk dalam masyarakat lapisan bawah. Kejahatan ini dapat dikategorikan kepada *white collar crime* (kejahatan kerah putih). Jo Ann L. Miller, mengkategorikan pelakunya menjadi 4 (empat).

(a) *Organizational occupational crime*
Pelakunya adalah para eksekutif. Mereka melakukan perbuatan ilegal atau merugikan orang lain melalui jaringan internet demi kepentingan atau keuntungan korporasi.

(b) *Government occupational crime*
Pelakunya adalah pejabat atau birokrat yang melakukan perbuatan ilegal melalui internet atas persetujuan atau perintah negara atau pemerintah, meski dalam banyak kasus, bila terungkap hal itu akan disangkal.

(c) *Professional occupational crime*
Berbagai profesi yang melakukan kejahatan secara sengaja (*malpractice*).

(d) *Individual occupational crime*
Perilaku menyimpang yang dilakukan oleh para pengusaha, pemilik modal atau orang-orang independen lainnya, walau mungkin tidak tinggi tingkat sosial ekonominya. Dalam bidang kerjanya kalangan ini memilih jalan yang menyimpang yang melanggar hukum atau merugikan orang lain.

Karakteristik "Cybercrime"

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain (CYBERCRIME_files\ inline_files\ SI10.HTM):

(1) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/ wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.

(2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.

(3) Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional

(4) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya

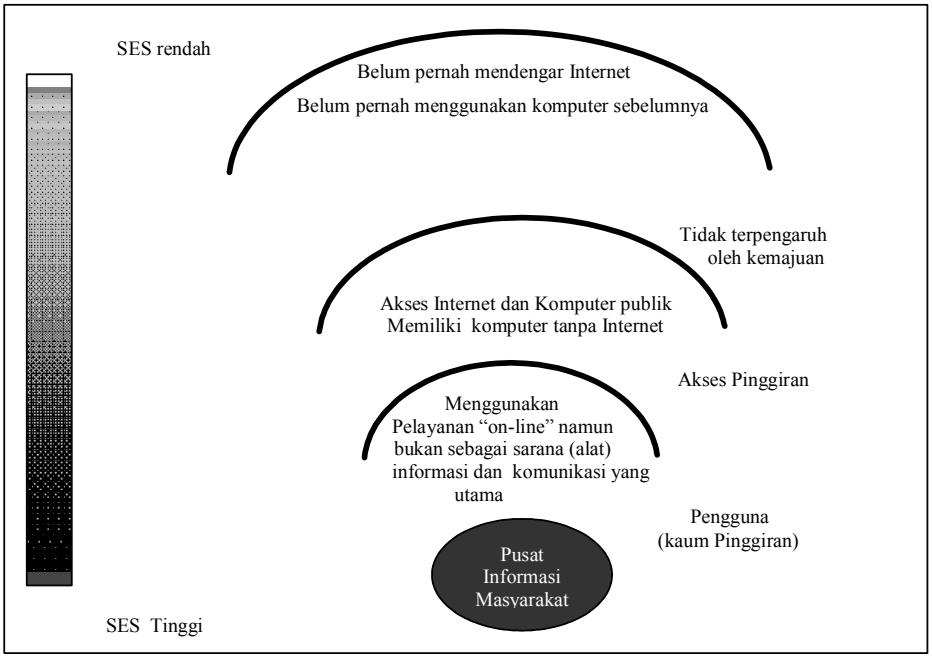
(5) Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

"Cybercrime" di Indonesia

Di antara negara berkembang, Indonesia termasuk negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia tidak memrioritaskan strategi pengembangan dan penguasaan teknologi. Yang terjadi kemudian, transfer teknologi dari negara maju tidak serta merta diikuti dengan penguasaan teknologi oleh negara berkembang seperti Indonesia. Bandingkan saja dengan Malaysia yang telah memproduksi secara massal *software*, per*sonal Computer* (PC), dan ponsel. Sungguh ironis memang, karena menjelang 1980-an Indonesia adalah negara Asia Tenggara pertama yang memiliki satelit komunikasi. Singapura dan Malaysia yang saat itu masih menyewa satelit Palapa dari Indonesia, kini menjadi negara maju berbasis teknologi komunikasi modern.

Meski masih diperdebatkan, dapat dikatakan Indonesia merupakan negara yang memiliki kesenjangan digital yang cukup lebar. Kesenjangan digital dapat diartikan sebagai adanya jurang di antara mereka yang mampu mengakses teknologi komunikasi dan yang tidak mampu (Staubhaar & La Rose, 2000:9). Selain masih senjangnya tingkat pendidikan dan ekonomi di Indonesia, kesempatan

Gambar 1: Model Pusat-Pinggiran Akses Teleteknologi



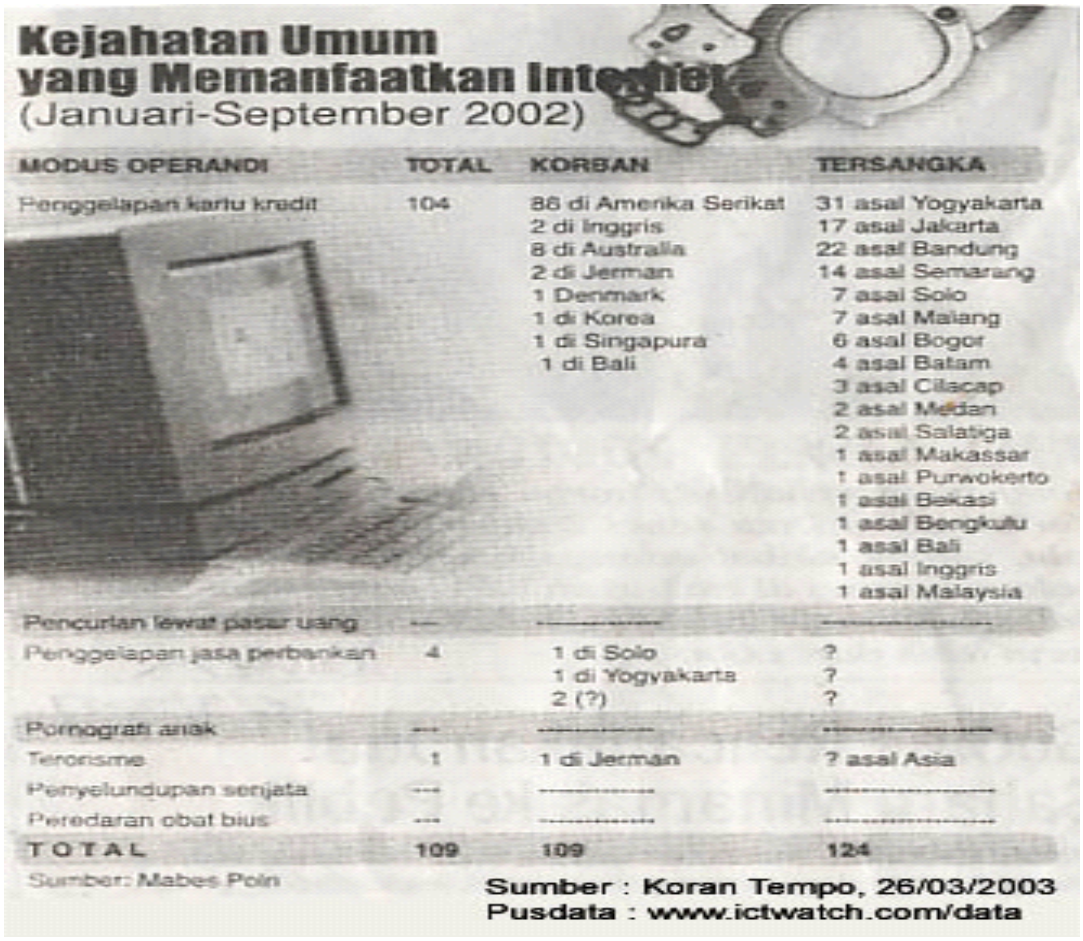
Sumber: Wilhelm (2003:119)

untuk menggunakan teknologi komunikasi di Indonesia belum merata. Ketimpangan, ketidakmilikan informasi dan telekomunikasi dapat dibagi dalam beberapa kategori. Yang paling banyak aksesnya, tentu saja, yang paling dekat dengan pusat informasi masyarakat.

Meskipun terdapat kesenjangan digital, di Indonesia marak sekali kejahatan *cyber*. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para *hacker* hitam. Mereka bisa memperoleh barang apa pun yang diinginkan, mulai dari berlian, radar laut, *corporate software*, *computer server*, Harley Davidson, hingga senjata M-16 (*Warta Ekonomi.com*, 23 Desember 2002) dengan menggunakan kartu kredit milik orang lain. Istilahnya adalah c*arding*. Para *carder* (*hacker* hitam) memesan barang-barang melalui internet untuk dikirimkan ke negara mereka berada. Barang yang dipesan dapat digunakan sendiri, dapat pula dijual dengan harga yang sangat murah. Misalnya, *Notebook* bermerk *Sony* seharga 20 Juta yang dipesan melalui *carding*, dijual seharga 4 Juta rupiah. Untuk yang satu ini, *ClearCommerce*, perusahaan keamanan internet yang berbasis di Texas, Amerika Serikat, memasukkan Indonesia ke dalam daftar negara-negara terburuk untuk kejahatan yang memanfaatkan kecanggihan teknologi komunikasi. Setidaknya, 20 persen transaksi kartu kredit internet yang berasal dari Indonesia merupakan penipuan. Berikut ini adalah data kejahatan yang memanfaatkan internet:

Dari data di bawah (*Koran Tempo*, 26 Maret 2003), Yogyakarta menempati urutan pertama dan Bandung kedua dalam *cybercrime* jenis *carding di* Indonesia. Yang melakukan jenis kejahatan itu adalah kalangan muda, biasanya mahasiswa. Seorang mahasiswa universitas swasta di Bandung pernah memesan 5 buah ponsel *Nokia Communicator* yang ia jual seharga 5 Juta rupiah, padahal saat itu harganya berkisar 10 Juta rupiah.

Gambar 2: Kejahatan Umum yang Memanfaatkan Internet



Kejahatan Umum yang Memanfaatkan Internet
(Januari-September 2002)

MODUS OPERANDI	TOTAL	KORBAN	TERSANGKA
Penggelapan kartu kredit	104	86 di Amerika Serikat 2 di Inggris 8 di Australia 2 di Jerman 1 Denmark 1 di Korea 1 di Singapura 1 di Bali	31 asal Yogyakarta 17 asal Jakarta 22 asal Bandung 14 asal Semarang 7 asal Solo 7 asal Malang 6 asal Bogor 4 asal Batam 3 asal Cilacap 2 asal Medan 2 asal Salatiga 1 asal Makassar 1 asal Purwokerto 1 asal Bekasi 1 asal Bengkulu 1 asal Bali 1 asal Inggris 1 asal Malaysia
Pencurian lewat pasar uang	---	----------	----------
Penggelapan jasa perbankan	4	1 di Solo 1 di Yogyakarta 2 (?)	? ? ?
Pornografi anak	---	----------	----------
Terorisme	1	1 di Jerman	? asal Asia
Penyelundupan senjata	---	----------	----------
Peredaran obat bius	---	----------	----------
TOTAL	109	109	124

Sumber: Mabes Polri

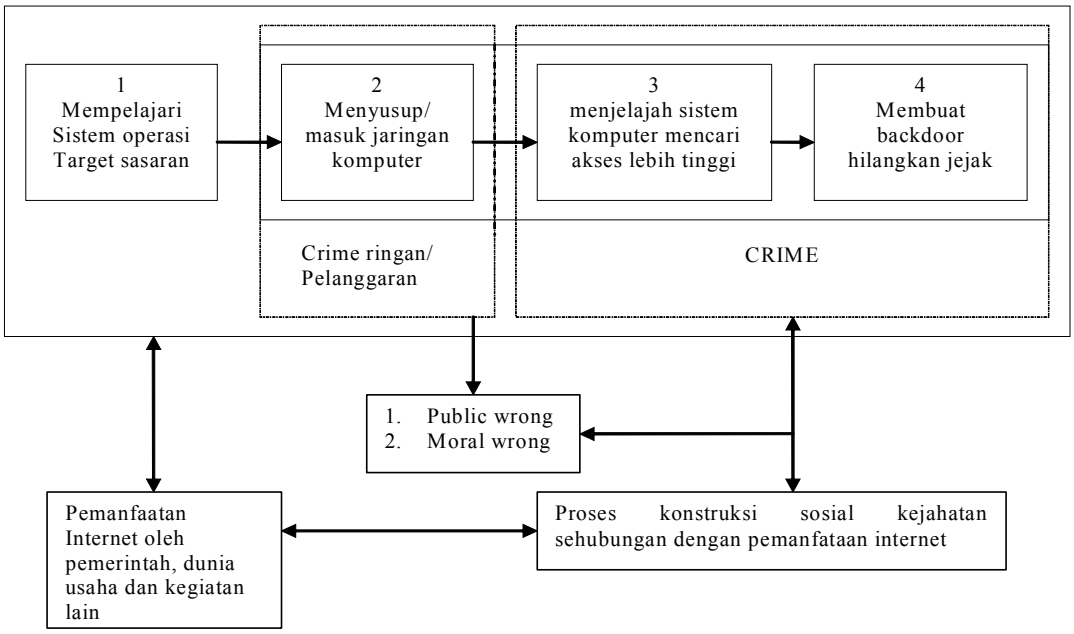
Sumber : Koran Tempo, 26/03/2003
Pusdata : www.ictwatch.com/data

Agar tidak diketahui identitasnya, ia melakukan *carding* di warnet sekitar kampus dan saat mengambil pesanan, agar dimudahkan, ia bekerjasama dan memberi sejumlah uang kepada oknum karyawan biro pengiriman paket terkemuka di Indonesia.

Indonesia tampaknya akan semakin mengukuhkan diri sebagai negara kampiun penipuan kartu kredit di internet Dalam berbagai urusan yang berkonotasi buruk, Indonesia memang seringkali termasuk di dalamnya, mulai dari pendapatan perkapita yang rendah, mutu pendidikan, tingkat korupsi, termasuk *cybercrime* jenis *carding*.

Kejahatan memang tidak dapat diprediksi kejadiannya, tidak mempedulikan tempat dan suasana ketika hendak muncul, tidak pula membanding-bandingkan siapa pelaku dan korbannya, tidak mengenal kasta ataupun status sosial pelaku dan korbannya. Saat muncul, ia dapat menjadi bahan yang menarik untuk dibicarakan, baik di media massa maupun ruang-ruang seminar. Apalagi saat kejahatan itu dipadukan dengan kecanggihan teknologi komunikasi. Tanpa sadar

Gambar 3. Bagan Konstruksi Kejahatan dari "Hacking"



Sumber: Raharjo (2002)

di sekeliling kita terdapat kejahatan yang "*innocent*", seolah tanpa dosa dan begitu halus.

Adapun konstruksi kejahatan *Hacking* dapat dilihat pada gambar 3.

Selain *cybercrime* jenis *carding*, di Indonesia juga sering terjadi kasus *deface*. Tampilan situs di Internet dirusak dan diganti oleh para *hacker* hitam. Berikut ini adalah kasus-kasus yang pernah terjadi (Raharjo, 202:35):

(a) Tahun 1997 ketika masalah Timor-Timur menghangat, situs milik Departemen Luar Negri dan ABRI (TNI, pen) dijebol oleh *craker Porto* (Portugis) yang pro-kemerdekaan. Mereka juga merusak situs-situs bisnis dan pendidikan. Serangan dari *craker* Porto ini mendapat balasan dari *craker* Indonesia. Hal ini dilakukan karena, menurut mereka, *craker* Porto dinilai keterlaluan, serangannya membabi-buta, tidak mempedulikan apakah itu situs milik pemerintah ataupun bukan, situs bisnis maupun situs pendidikan.
(b) Tahun 1998, tampilan depan atau *frontpage* Pusat Dokumentasi Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) diganti dengan gambar wanita telanjang.
(c) Tahun 1998, setelah kerusuhan 13–14 Mei, *craker* yang diduga berasal dari Cina menghantam situs milik pemerintah, yaitu BKKBN. Serangan ini merupakan reaksi atas pemberitaan media mengenai kerusuhan Mei yang menyebabkan etnis Cina di Indonesia menjadi korban pembantaian dan pemerkosaan.
(d) Juni 1999, *homepage* POLRI diganti dengan gambar telanjang, kemudian diganti lagi dengan gambar yang mirip logo PDI-Perjuangan.
(e) Januari 2000, situs yang diserang, antara lain Bursa Efek Jakarta (BEJ), Bank Central Asia dan Indosatnet.

(f) September dan Oktober 2000, Fabian Clone berhasil menjebol web milik Bank Bali, sebelumnya juga berhasil menjebol *web* milik Bank Lippo. Kedua bank itu memberikan layanan *Internet Banking*, kerugian yang diderita lebih besar dibandingkan kerugian yang diderirta BEJ.

(g) Januari 2001, situs milik PT. Ajinomoto Indonesia diserang *craker*. Serangan ini merupakan reaksi atas penggunaan *enzim porcine* (babi) yang digunakan sebagai katalis dalam proses pembuatan bumbu penyedap rasa. Situs Ajinomoto hhtp://www.mjk.ajinomoto.co.id ketika dibuka yang muncul adalah gambar seekor babi yang tengah tersenyum dengan tulisan *Babi, open in December 2K, "Ajinomoto You Lied to Us", "Ajinomoto: HARAM...HARAM...HARAM"*.

(h) Pada 8 Mei 2001, situs Polri mendapat serangan dari Kesatuan Aksi *Hacker* Muslim Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando Jihad.

Bila tidak ditangani dengan baik, ada kemungkinan jumlah kasus berikut korban akan bertambah, baik *cybercrime* dalam bentuk *carding* maupun *deface*, termasuk *cyberporn* meskipun tidak semua publik sepakat bahwa itu adalah suatu kejahatan. Namun, dapat dibayangkan bila orang-orang di sekitar kita, misalnya isteri dan anak kita yang tidak bersalah, tiba-tiba fotonya terpampang di internet dalam keadaan tanpa pakaian dengan teknik rekayasa foto melalui komputer.

Urgensi Penyelesaian "Cybercrime" di Indonesia

Berdasarkan berbagai kasus *cybercrime* yang telah terjadi dan pasti akan bertambah, perlu kiranya dilakukan percepatan dalam menuntaskan kasus *cybercrime*. Untuk menghadapi sekian banyak varian dan modifikasi modus kejahatan di Internet, maka langkah represif dan reaktif yang selama ini dilakukan oleh aparat penegak hukum tidaklah memadai. Aparat tidak siap menghadapinya. Maraknya *cybercrime* menunjukkan ketidakberdayaan pemerintah dalam menyelesaikannya. Oleh karena itu, pemerintah harus meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi, dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*. Aparat kepolisian perlu menanggapi secara serius kejahatan saiber.

Tentunya, harus dibarengi pula dengan serangkaian langkah proaktif dan antisipatif yang dilakukan oleh beragam institusi terkait di Indonesia. Misalnya, asosiasi yang membawahi para *Internet Service Provider* (ISP) dan warnet di Indonesia harus memikirkan langkah yang akan diambil untuk melindungi para konsumen.

Selanjutnya, adalah dengan melakukan kampanye dan edukasi tentang ber-internet yang aman secara komprehensif dan berkala kepada masyarakat umum. Jika hal tersebut tidak segera dilakukan, maka kita harus siap menerima kenyataan bahwa peningkatan penetrasi Internet di Indonesia akan berbanding lurus dengan meningkatnya angka kejahatan Internet secara kuantitatif dan kualitatif. Ujung-ujungnya, hal tersebut justru akan menghancurkan kegiatan usaha/bisnis dan industri internet di Indonesia. Seperti pemblokiran yang dilakukan komunitas internet internasional terhadap pengguna internet dengan nomor *Internet Provider* (IP) Indonesia, sehingga kegiatan bisnis di dunia *cyber* tidak mungkin dilakukan. Itu semua akan menghancurkan kegiatan ekonomi melalui internet.

Tidak kalah pentingnya pula, pemerintah harus bergegas membuat UU *Cyberlaw* untuk menuntaskan kasus *cybercrime*. Perlu dipahami bahwa kegiatan bisnis melalui internet telah mengubah tatanan ekonomi konvesional. Hal itu memunculkan ketidakpastian, karena pihak yang berkomunikasi tidak bertemu secara tatap muka. Untuk memberikan kepastian, perlu dilindungi oleh *cyberlaw*. Meskipun pengguna internet di Indonesia kurang dari 5 % total populasi penduduk (data lainnya menyebutkan hanya 1,9 % atau sekitar 4,38 juta), *cyberlaw* tetap diperlukan sebagai pegangan hukum bagi aparat dalam menuntaskan *cybercrime*. Akan lebih buruk bila tak ada perangkat hukum yang memadai.

Daftar Pustaka

A. Buku

Mahayana, Dimitri. 1999. *Menjemput Masa Depan*, Bandung: PT. Remaja Rosdakarya.

Naisbitt, John, Naisbitt, Nana, & Philips, Douglas. 2001. *High Tech High Touch*. Bandung: Mizan Pustaka.

Piliang, Yasraf Amir. 2001. *Sebuah Dunia yang Menakutkan*. Bandung: Mizan Pustaka.

Raharjo, Agus. 2002. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*. Bandung: Citra Aditya Bakti.

Staubhaar, J. & La Rose, R., *Media Now,* 2000.

Temporal, Paul, K.C. Lee. 2001. *Hi-Tech Hi Touch Branding*. Jakarta: Salemba Empat.

Ustadiyanto, Riyeke. 2001. *Framework e-Commerce*. Yogyakarta: Andi

Wilhelm, Anthony G, *Demokrasi di Era Digital*. 2003. Yogyakarta: Pustaka Pelajar.

B. Sumber lain:

Kompas Cyber Media, 05 Mei 2002.

Republika, 22 Agustus 1999.

komputeraktif, No. 43/18 Desember 2002.

Cybercrime_files\inline_files\SI10.HTM.

Warta Ekonomi.com, 23 Desember 2002.

Terakreditasi Dirjen Dikti SK No. 56/DIKTI/Kep/2005

"Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia

M.E. Fuady

ABSTRACT

It had been long known that technology, as Janus, has two side of coins: the good side, and the bad side. Everybody knows the benefit of technology development. But there aren't much who realize the negative potent of technology. Cybercrime discussed in this article is an example of how crime was developed sophisticatedly by using technological means. Cybercrime, simply defined as criminal acts using cyber and Internet, has faced a new challenge for lawmaker and law enforcement mission. In Indonesia, carding become serious issues to be combated. Another type of cybercrime frequently occur in Indonesia are hacking and deface. Although Internet user in Indonesia is estimated no more than 5% of total population (4.38 million persons), everybody must attended cybercrime issues seriously. The loss of cybercrime reached unspeakable heights and damaged public safety in communication and information flows.

Kata kunci: "cybercrime", realitas virtual, dunia tanpa batas

Internet: Teknologi Pencipta Dunia "Cyber"

Kehadiran teknologi komunikasi modern seperti internet telah membuat pandangan manusia mengenai kehidupan berubah. Paradigma komunikasi manusia dalam menjalani aktivitas ekonomi, bisnis, interaksi sosial, dan politik, menjadi berbeda. Sebelumnya, manusia didominasi oleh aktivitas yang bersifat fisik, *face to face*. Manusia dihalangi oleh berbagai keterbatasan. Dengan internet, ruang, jarak, dan waktu yang membatasi manusia menghilang. Menurut Kenichi Ohmae (Mahayana, 1999:97), itulah dunia tanpa batas (*the borderless world*).

Internet merupakan jaringan dari jutaan komputer yang saling terhubungkan. Dengan internet, setiap orang di seluruh dunia dapat berkomunikasi hanya dengan menekan *keyboard* dan *mouse* di hadapannya. Informasi apa pun yang dibutuhkan telah tersedia. Karena kemudahan yang ditawarkan itulah banyak individu yang menggunakannya. Dibandingkan radio dan televisi, penetrasi internet di kalangan masyarakat, termasuk yang paling cepat. Untuk mencapai pengguna sebanyak 50 juta orang, internet hanya membutuhkan waktu 5 tahun, sementara radio membutuhkan waktu 38 tahun dan televisi 13 tahun (Temporal & Lee, 2002:7). Saat ini, diperkirakan pengguna internet telah mencapai 220 juta orang.

Dengan menggunakan internet, *user* berkesempatan untuk berpetualang, berkelana, berselancar menelusuri *cyberspace*, sebuah dunia komunikasi berbasis komputer (*computer mediated communication*). Realitas yang ditawarkan adalah realitas virtual, kehadirannya tidak dapat ditangkap

atau dipegang tangan, tetapi dikonstruksikan secara sosial oleh orang-orang yang menggeluti teknologi komunikasi dan informasi. Realitas *cyberspace* adalah kenyataan yang melampaui dan artifisial (*hyperreal*). Menurut Piliang (2001), karena rekayasa sedemikian rupa, kenyataan (*real*) ditutupi oleh tanda kenyataan (*sign of real*) sedemikian rupa, sehingga antara tanda dan relitas, antara model dan kenyataan, tidak lagi dapat dibedakan.

Cyberspace menawarkan segala hal yang diperlukan manusia, termasuk kesenangan, keuntungan, dan kemudahan tanpa bersusah payah menggerakkan badan untuk memeroleh sesuatu. Berbagai informasi gratis dari surat kabar dalam dan luar negeri dapat diperoleh tanpa membeli. Menikmati musik tanpa harus membeli kaset. Bagi dosen, berbagai literatur tersaji secara gratis tanpa harus pergi ke tempat berada. Inilah "zona mabuk teknologi" yang dikemukakan Philips dan Naisbitt (2001).

Kehidupan virtual yang disajikan *cyberspace* telah memunculkan bentuk aktivitas baru untuk mencapai kepuasan, seperti *teleshopping*, *teleconference*, *virtual gallery*, *virtual museum*, *e-commerce*, namun juga memunculkan penyimpangan-penyimpangan seperti kejahatan dengan memanfaatkan internet atau *cybercrime*.

"Cybercrime": Bentuk Kejahatan di Dunia Maya

Dalam beberapa literatur, *cybercrime* sering diidentikkan sebagai *computer crime. The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai:"…*any illegal act requiring knowledge of 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*". Hamzah (1989) mengartikan: "kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal".

Dari beberapa pengertian di atas, Wisnubroto (1999) merumuskan *computer crime* sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Secara ringkas, *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi komputer yang canggih. Selanjutnya, disebabkan kejahatan itu dilakukan di ruang *cyber* melalui internet, muncul istilah *cybercrime*.

Bagi sebagian besar masyarakat yang terbiasa menggunakan media teknologi komunikasi (telekomunikasi), *cybercrime* bukanlah istilah yang asing terdengar. *Cybercrime* atau kejahatan di ruang maya merupakan sebuah fenomena yang tidak terbantahkan. Tidak terlihat namun nyata. Terdapat berbagai kasus *cybercrime* yang kian hari kian meningkat, terutama di negara-negara yang tidak memiliki kepastian hukum dalam bidang teknologi komunikasi modern (*convergence*).

Teknologi komunikasi yang memiliki kekuatan dahsyat dalam merubah perilaku komunikasi manusia, selain membawa keuntungan berupa kemudahan dalam berkomunikasi, ternyata memiliki "sisi gelap". Teknologi membawa kerugian, salah satunya berupa semakin dipermudahkannya "penjahat" dalam melakukan kejahatannya. Kecanggihan teknologi memungkinkan penjahat *cyber* memangsa korban-korbannya. Meski tidak mau disebut sebagai pelaku kriminal, sebagai akibat dari perbuatannya, mereka tidak ada bedanya dengan seorang penjahat.

Menurut Raharjo (2002:29), sebagai sebuah gejala sosial, kejahatan telah ada sejak awal kehidupan manusia di dunia, namun kemajuan teknologi komunikasi membuat kejahatan dalam bentuk primitif berubah menjadi sebuah kejahatan yang lebih maju (modern). Kejahatan konvensional di dunia nyata muncul dalam dunia maya (*virtual*) dengan wajah kejahatan yang telah diperhalus sedemikian rupa. Kehalusan kejahatan virtual atau *cybercrime* membuat masyarakat luas, khususnya di negara berkembang yang memiliki kesenjangan digital seperti Indonesia, tidak merasakannya sebagai sebuah bentuk kejahatan. Padahal, sudah begitu banyak korban (*victim*) dan

kerugian moril dan materil akibat *cybercrime*. Korbannya dapat berupa *netizen* (penduduk dunia *virtual*/penghuni *cyberspace*) dan masyarakat luas yang awam.

Perusahaan yang bergerak dalam bidang bisnis dan individu tak berdosa, yang tidak memiliki keahlian bahkan pemahaman akan teknologi komunikasi, dapat menjadi korban. Tidak perlu jauh-jauh, kita semua masih ingat dengan kasus mahasiswa dan artis "bugil" yang beredar di internet. Sedikit sekali di antara mereka yang memahami teknologi komunikasi, tetapi mereka telah menjadi korban. Sebut saja artis dengan inisial YS, KD, KF, CK, dan masih banyak lagi. Itu salah satu contoh kecil korban dari *cybercrime*. Meski memang ada publik yang tidak menyepakati *cyberporn* sebagai *cybercrime*. Tetapi, kita telah melihat adanya korban akibat perbuatan pelaku *cybercrime*. Sebagai catatan penting, menurut Menteri Negara Komunikasi dan Informasi, sekitar 50 persen kalangan muda yang menggunakan internet lebih suka untuk mengunjungi situs porno (*Kompas Cyber Media*, 05 Mei 2002).

Untuk memahami *cybercrime*, perlu kiranya dipahami terlebih dahulu apa yang disebut dengan *hacker*, *cracker* dan beberapa lainnya. Karena, seperti halnya kehidupan nyata, ada di antara mereka yang "hitam" dan "putih", ada yang berlaku seperti pahlawan dan penjahat.

(1) *Hacker*

Hacker secara harfiah berarti mencincang atau membacok. Dalam arti luas adalah mereka yang menyusup melalui komputer ke dalam jaringan komputer (*Republika*, 22 Agustus 1999). Menurut Ustadiyanto (2001:304), ada definisi yang relevan, yakni *hacker* adalah orang-orang yang ahli dalam bidangnya. Bila komputer, maka dia pandai menggunakannya. Ia sangat menguasai komputer. *Hacker* adalah orang-orang yang gemar mempelajari seluk-beluk sistem komputer dan bereksperimen dengannya. Mereka pandai untuk menyusup ke dalam jaringan komunikasi suatu institusi di dunia maya. *Hacker* menjunjung tinggi etika atau norma yang berlaku di dunia maya. Mereka anti penyensoran, anti penipuan, dan pemaksaan kehendak pada orang lain. Mereka memegang prinsip bahwa meng-*hack* untuk tujuan meningkatkan keamanan jaringan internet. Misalnya, bila ada sebuah perusahaan perbankan mengatakan bahwa jaringan sistem komunikasi mereka sudah sangat canggih dan mustahil dibobol, tidak dapat ditembus oleh siapa pun, maka *hacker* tertantang untuk mencoba dan setelah berhasil mereka memperingatkan betapa lemahnya sistem informasi perusahaan terrsebut. Oleh karena itu, tidak sedikit dari mereka yang akhirnya direkrut perusahaan untuk mengamankan sistem informasi dan komunikasi di dunia maya.

(2) *Cracker*

Di dunia *cyber*, ada pula *hacker* yang memiki sisi gelap. Mereka disebut *cracker*. Para *cracker* ini secara ilegal melakukan penyusupan dan perusakan terhadap situs, *website,* dan sistem keamanan jaringan internet untuk memperoleh kesenangan dan keuntungan. Mereka bangga dan sombong atas keberhasilan mereka merusak situs sebuah perusahaan. Serangannya sangat luar biasa. Kementerian Petahanan Amerika Serikat di Pentagon mencatat serangan 100 *cracker* dalam satu hari (*Republika*, 6 Januari 2000).

(3) *Carder*

Carder adalah orang yang melakukan *cracking*, yakni pembobolan terhadap kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk kepentingan pribadi. Biasanya yang menjadi korbannya adalah mereka yang memiliki kartu kredit dalam jumlah besar. Menurut hasil riset, pada tahun 2002, Indonesia menempati urutan kedua setelah Ukraina dalam kejahatan *carding*.

(4) *Deface*

Deface adalah tindakan menyusup ke suatu situs, lalu mengubah tampilan halaman dari situs dengan tujuan tertentu. Indonesia pernah diserang para *deface* yang mengubah situs TNI. Tampilan gambar Burung Garuda Pancasila diganti dengan lambang palu arit. *Hompage* Polri diganti tampilannya dengan

gambar wanita telanjang.

(5) *Phreaker*
*Yaitu ses*eorang yang melakukan *cracking* terhadap jaringan telepon, sehingga dapat menelepon secara gratis ke daerah manapun yang dituju (*Komputeraktif*, No. 43/18 Desember 2002). Di Indonesia, kasus semacam ini pernah terjadi pada wartel–wartel.

Para pelaku *hacking* biasanya bukan dari kalangan lapisan bawah, pada umumnya mereka adalah kaum terpelajar, setidak-tidaknya mengenyam pendidikan formal sampai tingkat tertentu dan dapat menggunakan atau mengoperasikan komputer. Para *craker* adalah orang yang berpendidikan, tidak buta teknologi, secara ekonomis mampu dan tidak termasuk dalam masyarakat lapisan bawah. Kejahatan ini dapat dikategorikan kepada *white collar crime* (kejahatan kerah putih). Jo Ann L. Miller, mengkategorikan pelakunya menjadi 4 (empat).

(a) *Organizational occupational crime*
Pelakunya adalah para eksekutif. Mereka melakukan perbuatan ilegal atau merugikan orang lain melalui jaringan internet demi kepentingan atau keuntungan korporasi.

(b) *Government occupational crime*
Pelakunya adalah pejabat atau birokrat yang melakukan perbuatan ilegal melalui internet atas persetujuan atau perintah negara atau pemerintah, meski dalam banyak kasus, bila terungkap hal itu akan disangkal.

(c) *Professional occupational crime*
Berbagai profesi yang melakukan kejahatan secara sengaja (*malpractice*).

(d) *Individual occupational crime*
Perilaku menyimpang yang dilakukan oleh para pengusaha, pemilik modal atau orang-orang independen lainnya, walau mungkin tidak tinggi tingkat sosial ekonominya. Dalam bidang kerjanya kalangan ini memilih jalan yang menyimpang yang melanggar hukum atau merugikan orang lain.

Karakteristik "Cybercrime"

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain (CYBERCRIME_files\ inline_files\ SI10.HTM):

(1) Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/ wilayah maya (*cyberspace*), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.

(2) Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet.

(3) Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional

(4) Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya

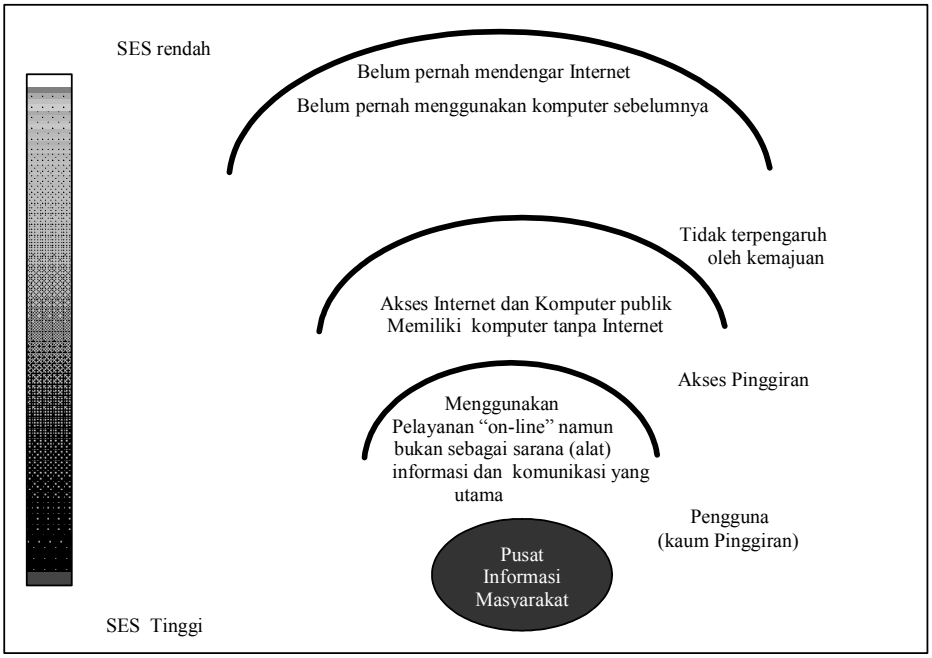
(5) Perbuatan tersebut seringkali dilakukan secara transnasional/melintasi batas negara.

"Cybercrime" di Indonesia

Di antara negara berkembang, Indonesia termasuk negara yang lambat mengikuti perkembangan teknologi komunikasi modern. Indonesia tidak memrioritaskan strategi pengembangan dan penguasaan teknologi. Yang terjadi kemudian, transfer teknologi dari negara maju tidak serta merta diikuti dengan penguasaan teknologi oleh negara berkembang seperti Indonesia. Bandingkan saja dengan Malaysia yang telah memproduksi secara massal *software*, per*sonal Computer* (PC), dan ponsel. Sungguh ironis memang, karena menjelang 1980-an Indonesia adalah negara Asia Tenggara pertama yang memiliki satelit komunikasi. Singapura dan Malaysia yang saat itu masih menyewa satelit Palapa dari Indonesia, kini menjadi negara maju berbasis teknologi komunikasi modern.

Meski masih diperdebatkan, dapat dikatakan Indonesia merupakan negara yang memiliki kesenjangan digital yang cukup lebar. Kesenjangan digital dapat diartikan sebagai adanya jurang di antara mereka yang mampu mengakses teknologi komunikasi dan yang tidak mampu (Staubhaar & La Rose, 2000:9). Selain masih senjangnya tingkat pendidikan dan ekonomi di Indonesia, kesempatan

Gambar 1: Model Pusat-Pinggiran Akses Teleteknologi



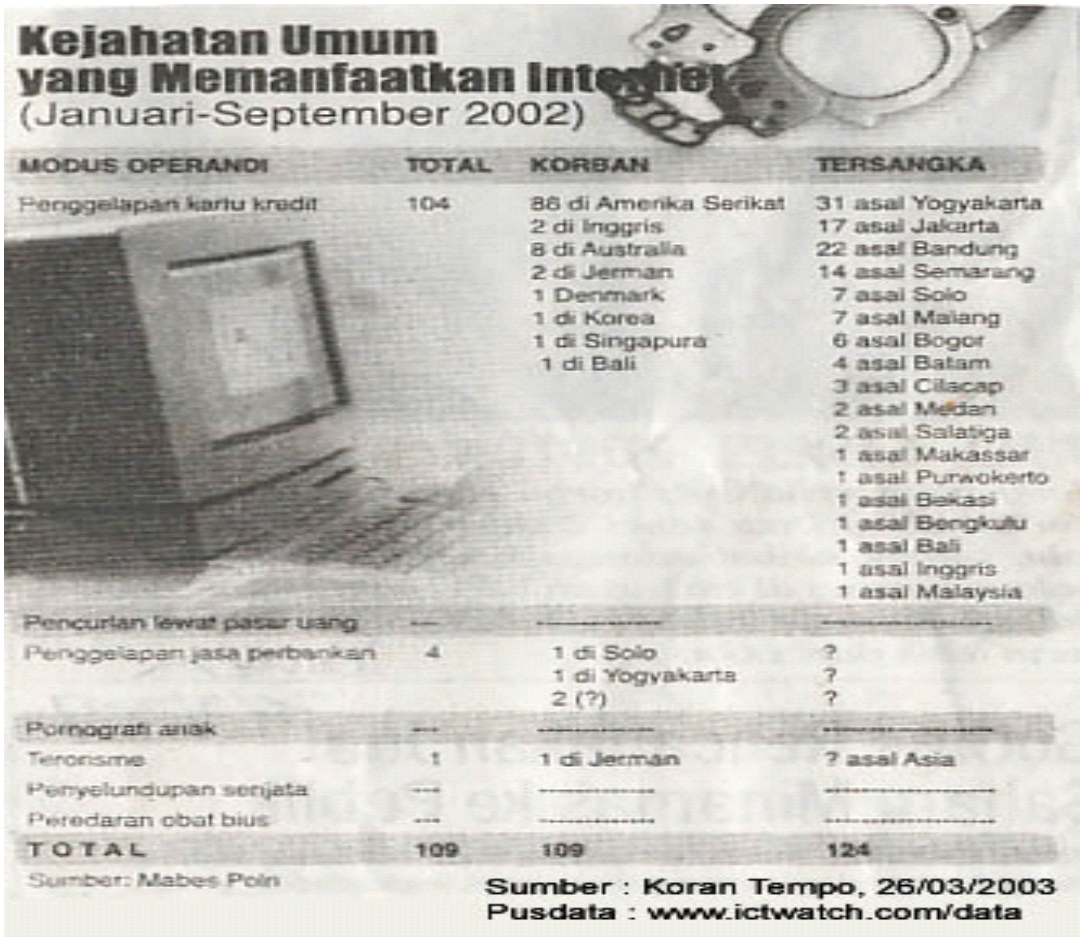
Sumber: Wilhelm (2003:119)

untuk menggunakan teknologi komunikasi di Indonesia belum merata. Ketimpangan, ketidakmilikan informasi dan telekomunikasi dapat dibagi dalam beberapa kategori. Yang paling banyak aksesnya, tentu saja, yang paling dekat dengan pusat informasi masyarakat.

Meskipun terdapat kesenjangan digital, di Indonesia marak sekali kejahatan *cyber*. Kasus yang paling sering terjadi adalah pembobolan kartu kredit oleh para *hacker* hitam. Mereka bisa memperoleh barang apa pun yang diinginkan, mulai dari berlian, radar laut, *corporate software*, *computer server*, Harley Davidson, hingga senjata M-16 (*Warta Ekonomi.com*, 23 Desember 2002) dengan menggunakan kartu kredit milik orang lain. Istilahnya adalah c*arding*. Para *carder* (*hacker* hitam) memesan barang-barang melalui internet untuk dikirimkan ke negara mereka berada. Barang yang dipesan dapat digunakan sendiri, dapat pula dijual dengan harga yang sangat murah. Misalnya, *Notebook* bermerk *Sony* seharga 20 Juta yang dipesan melalui *carding*, dijual seharga 4 Juta rupiah. Untuk yang satu ini, *ClearCommerce*, perusahaan keamanan internet yang berbasis di Texas, Amerika Serikat, memasukkan Indonesia ke dalam daftar negara-negara terburuk untuk kejahatan yang memanfaatkan kecanggihan teknologi komunikasi. Setidaknya, 20 persen transaksi kartu kredit internet yang berasal dari Indonesia merupakan penipuan. Berikut ini adalah data kejahatan yang memanfaatkan internet:

Dari data di bawah (*Koran Tempo*, 26 Maret 2003), Yogyakarta menempati urutan pertama dan Bandung kedua dalam *cybercrime* jenis *carding di* Indonesia. Yang melakukan jenis kejahatan itu adalah kalangan muda, biasanya mahasiswa. Seorang mahasiswa universitas swasta di Bandung pernah memesan 5 buah ponsel *Nokia Communicator* yang ia jual seharga 5 Juta rupiah, padahal saat itu harganya berkisar 10 Juta rupiah.

Gambar 2: Kejahatan Umum yang Memanfaatkan Internet



Kejahatan Umum yang Memanfaatkan Internet
(Januari-September 2002)

MODUS OPERANDI	TOTAL	KORBAN	TERSANGKA
Penggelapan kartu kredit	104	86 di Amerika Serikat 2 di Inggris 8 di Australia 2 di Jerman 1 Denmark 1 di Korea 1 di Singapura 1 di Bali	31 asal Yogyakarta 17 asal Jakarta 22 asal Bandung 14 asal Semarang 7 asal Solo 7 asal Malang 6 asal Bogor 4 asal Batam 3 asal Cilacap 2 asal Medan 2 asal Salatiga 1 asal Makassar 1 asal Purwokerto 1 asal Bekasi 1 asal Bengkulu 1 asal Bali 1 asal Inggris 1 asal Malaysia
Pencurian lewat pasar uang	---	----------	----------
Penggelapan jasa perbankan	4	1 di Solo 1 di Yogyakarta 2 (?)	? ? ?
Pornografi anak	---	----------	----------
Terorisme	1	1 di Jerman	? asal Asia
Penyelundupan senjata	---	----------	----------
Peredaran obat bius	---	----------	----------
TOTAL	109	109	124

Sumber: Mabes Polri

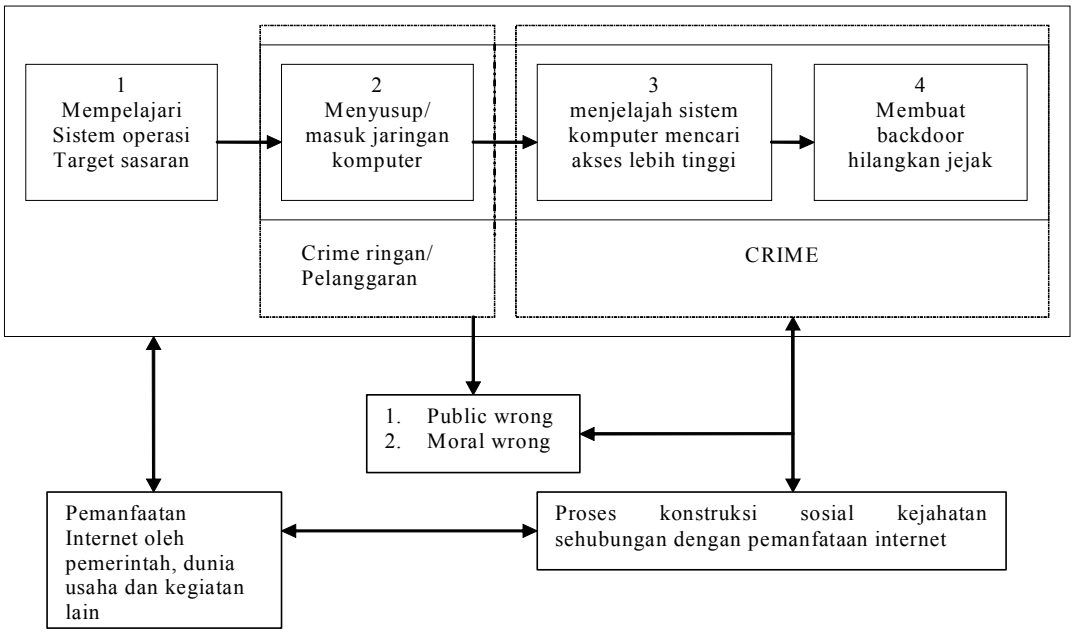
Sumber : Koran Tempo, 26/03/2003
Pusdata : www.ictwatch.com/data

Agar tidak diketahui identitasnya, ia melakukan *carding* di warnet sekitar kampus dan saat mengambil pesanan, agar dimudahkan, ia bekerjasama dan memberi sejumlah uang kepada oknum karyawan biro pengiriman paket terkemuka di Indonesia.

Indonesia tampaknya akan semakin mengukuhkan diri sebagai negara kampiun penipuan kartu kredit di internet Dalam berbagai urusan yang berkonotasi buruk, Indonesia memang seringkali termasuk di dalamnya, mulai dari pendapatan perkapita yang rendah, mutu pendidikan, tingkat korupsi, termasuk *cybercrime* jenis *carding*.

Kejahatan memang tidak dapat diprediksi kejadiannya, tidak mempedulikan tempat dan suasana ketika hendak muncul, tidak pula membanding-bandingkan siapa pelaku dan korbannya, tidak mengenal kasta ataupun status sosial pelaku dan korbannya. Saat muncul, ia dapat menjadi bahan yang menarik untuk dibicarakan, baik di media massa maupun ruang-ruang seminar. Apalagi saat kejahatan itu dipadukan dengan kecanggihan teknologi komunikasi. Tanpa sadar

Gambar 3. Bagan Konstruksi Kejahatan dari "Hacking"



Sumber: Raharjo (2002)

di sekeliling kita terdapat kejahatan yang "*innocent*", seolah tanpa dosa dan begitu halus.

Adapun konstruksi kejahatan *Hacking* dapat dilihat pada gambar 3.

Selain *cybercrime* jenis *carding*, di Indonesia juga sering terjadi kasus *deface*. Tampilan situs di Internet dirusak dan diganti oleh para *hacker* hitam. Berikut ini adalah kasus-kasus yang pernah terjadi (Raharjo, 202:35):

(a) Tahun 1997 ketika masalah Timor-Timur menghangat, situs milik Departemen Luar Negri dan ABRI (TNI, pen) dijebol oleh *craker Porto* (Portugis) yang pro-kemerdekaan. Mereka juga merusak situs-situs bisnis dan pendidikan. Serangan dari *craker* Porto ini mendapat balasan dari *craker* Indonesia. Hal ini dilakukan karena, menurut mereka, *craker* Porto dinilai keterlaluan, serangannya membabi-buta, tidak mempedulikan apakah itu situs milik pemerintah ataupun bukan, situs bisnis maupun situs pendidikan.
(b) Tahun 1998, tampilan depan atau *frontpage* Pusat Dokumentasi Informasi Ilmiah Lembaga Ilmu Pengetahuan Indonesia (PDII LIPI) diganti dengan gambar wanita telanjang.
(c) Tahun 1998, setelah kerusuhan 13–14 Mei, *craker* yang diduga berasal dari Cina menghantam situs milik pemerintah, yaitu BKKBN. Serangan ini merupakan reaksi atas pemberitaan media mengenai kerusuhan Mei yang menyebabkan etnis Cina di Indonesia menjadi korban pembantaian dan pemerkosaan.
(d) Juni 1999, *homepage* POLRI diganti dengan gambar telanjang, kemudian diganti lagi dengan gambar yang mirip logo PDI-Perjuangan.
(e) Januari 2000, situs yang diserang, antara lain Bursa Efek Jakarta (BEJ), Bank Central Asia dan Indosatnet.

(f) September dan Oktober 2000, Fabian Clone berhasil menjebol web milik Bank Bali, sebelumnya juga berhasil menjebol *web* milik Bank Lippo. Kedua bank itu memberikan layanan *Internet Banking*, kerugian yang diderita lebih besar dibandingkan kerugian yang diderirta BEJ.

(g) Januari 2001, situs milik PT. Ajinomoto Indonesia diserang *craker*. Serangan ini merupakan reaksi atas penggunaan *enzim porcine* (babi) yang digunakan sebagai katalis dalam proses pembuatan bumbu penyedap rasa. Situs Ajinomoto hhtp://www.mjk.ajinomoto.co.id ketika dibuka yang muncul adalah gambar seekor babi yang tengah tersenyum dengan tulisan *Babi, open in December 2K, "Ajinomoto You Lied to Us", "Ajinomoto: HARAM...HARAM...HARAM"*.

(h) Pada 8 Mei 2001, situs Polri mendapat serangan dari Kesatuan Aksi *Hacker* Muslim Indonesia (KAHMI). Serangan ini merupakan reaksi atas ditangkapnya pimpinan dari Pasukan Komando Jihad.

Bila tidak ditangani dengan baik, ada kemungkinan jumlah kasus berikut korban akan bertambah, baik *cybercrime* dalam bentuk *carding* maupun *deface*, termasuk *cyberporn* meskipun tidak semua publik sepakat bahwa itu adalah suatu kejahatan. Namun, dapat dibayangkan bila orang-orang di sekitar kita, misalnya isteri dan anak kita yang tidak bersalah, tiba-tiba fotonya terpampang di internet dalam keadaan tanpa pakaian dengan teknik rekayasa foto melalui komputer.

Urgensi Penyelesaian "Cybercrime" di Indonesia

Berdasarkan berbagai kasus *cybercrime* yang telah terjadi dan pasti akan bertambah, perlu kiranya dilakukan percepatan dalam menuntaskan kasus *cybercrime*. Untuk menghadapi sekian banyak varian dan modifikasi modus kejahatan di Internet, maka langkah represif dan reaktif yang selama ini dilakukan oleh aparat penegak hukum tidaklah memadai. Aparat tidak siap menghadapinya. Maraknya *cybercrime* menunjukkan ketidakberdayaan pemerintah dalam menyelesaikannya. Oleh karena itu, pemerintah harus meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi, dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*. Aparat kepolisian perlu menanggapi secara serius kejahatan saiber.

Tentunya, harus dibarengi pula dengan serangkaian langkah proaktif dan antisipatif yang dilakukan oleh beragam institusi terkait di Indonesia. Misalnya, asosiasi yang membawahi para *Internet Service Provider* (ISP) dan warnet di Indonesia harus memikirkan langkah yang akan diambil untuk melindungi para konsumen.

Selanjutnya, adalah dengan melakukan kampanye dan edukasi tentang ber-internet yang aman secara komprehensif dan berkala kepada masyarakat umum. Jika hal tersebut tidak segera dilakukan, maka kita harus siap menerima kenyataan bahwa peningkatan penetrasi Internet di Indonesia akan berbanding lurus dengan meningkatnya angka kejahatan Internet secara kuantitatif dan kualitatif. Ujung-ujungnya, hal tersebut justru akan menghancurkan kegiatan usaha/bisnis dan industri internet di Indonesia. Seperti pemblokiran yang dilakukan komunitas internet internasional terhadap pengguna internet dengan nomor *Internet Provider* (IP) Indonesia, sehingga kegiatan bisnis di dunia *cyber* tidak mungkin dilakukan. Itu semua akan menghancurkan kegiatan ekonomi melalui internet.

Tidak kalah pentingnya pula, pemerintah harus bergegas membuat UU *Cyberlaw* untuk menuntaskan kasus *cybercrime*. Perlu dipahami bahwa kegiatan bisnis melalui internet telah mengubah tatanan ekonomi konvesional. Hal itu memunculkan ketidakpastian, karena pihak yang berkomunikasi tidak bertemu secara tatap muka. Untuk memberikan kepastian, perlu dilindungi oleh *cyberlaw*. Meskipun pengguna internet di Indonesia kurang dari 5 % total populasi penduduk (data lainnya menyebutkan hanya 1,9 % atau sekitar 4,38 juta), *cyberlaw* tetap diperlukan sebagai pegangan hukum bagi aparat dalam menuntaskan *cybercrime*. Akan lebih buruk bila tak ada perangkat hukum yang memadai.

Daftar Pustaka

A. Buku

Mahayana, Dimitri. 1999. *Menjemput Masa Depan*, Bandung: PT. Remaja Rosdakarya.

Naisbitt, John, Naisbitt, Nana, & Philips, Douglas. 2001. *High Tech High Touch*. Bandung: Mizan Pustaka.

Piliang, Yasraf Amir. 2001. *Sebuah Dunia yang Menakutkan*. Bandung: Mizan Pustaka.

Raharjo, Agus. 2002. *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi Tinggi*. Bandung: Citra Aditya Bakti.

Staubhaar, J. & La Rose, R., *Media Now,* 2000.

Temporal, Paul, K.C. Lee. 2001. *Hi-Tech Hi Touch Branding*. Jakarta: Salemba Empat.

Ustadiyanto, Riyeke. 2001. *Framework e-Commerce*. Yogyakarta: Andi

Wilhelm, Anthony G, *Demokrasi di Era Digital*. 2003. Yogyakarta: Pustaka Pelajar.

B. Sumber lain:

Kompas Cyber Media, 05 Mei 2002.

Republika, 22 Agustus 1999.

komputeraktif, No. 43/18 Desember 2002.

Cybercrime_files\inline_files\SI10.HTM.

Warta Ekonomi.com, 23 Desember 2002.