

PERKEMBANGAN *CYBERCRIME* DAN UPAYA PENANGANANNYA DI INDONESIA OLEH POLRI^{*)}

Oleh : Kombes (Pol) Drs. Petrus Reinhard Golose, M.M¹

PENDAHULUAN

Kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dengan Internet dalam segala bidang seperti *e-banking*, *e-commerce*, *e-government*, *e-education* dan banyak lagi telah menjadi sesuatu yang lumrah. Bahkan apabila masyarakat terutama yang hidup di kota besar tidak bersentuhan dengan persoalan teknologi informasi dapat dipandang terbelakang atau "GAPTEK".

Internet telah menciptakan dunia baru yang dinamakan **cyberspace**² yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk *virtual* (tidak langsung dan tidak nyata). Walaupun

dilakukan secara virtual, kita dapat merasa seolah-olah ada di tempat tersebut dan melakukan hal-hal yang dilakukan secara nyata, misalnya bertransaksi, berdiskusi dan banyak lagi, seperti yang dikatakan oleh Gibson³ yang memunculkan istilah tersebut pertama kali dalam novelnya:

"A Consensual hallucination experienced daily billions of legitimate operators, in every nation...A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding".

Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif kita semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi ini,

^{*)} Makalah disampaikan dalam Seminar Nasional Mengenai "Penanganan *Cybercrime* di Indonesia ke arah Pengembangan Kebijakan yang Menyeluruh dan Terpadu", diselenggarakan di Menara Sjafruddin Prawiranegara Kompleks Perkantoran Bank Indonesia Jakarta, 10 Agustus 2006.

¹ Kepala Unit V IT/*Cybercrime*, Direktorat II Ekonomi Khusus Bareskrim Polri.

² Agus Rahardjo, *Cybercrime* pemahaman dan upaya pencegahan kejahatan berteknologi, (Bandung: PT Citra Aditya Bakti, 2002)

³ William Gibson, *Neuromancer* (New York: Ace, 1984)

misalnya kita dapat melakukan transaksi perbankan kapan saja dengan *e-banking*, *e-commerce* juga membuat kita mudah melakukan pembelian maupun penjualan suatu barang tanpa mengenal tempat. Mencari referensi atau informasi mengenai ilmu pengetahuan juga bukan hal yang sulit dengan adanya *e-library* dan banyak lagi kemudahan yang didapatkan dengan perkembangan Internet.

Tentunya, tidak dapat dipungkiri bahwa teknologi Internet membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat dilakukan dengan menggunakan media komputer secara *online* dengan risiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara disamping menimbulkan kejahatan-kejahatan baru.

Banyaknya dampak negatif yang timbul dan berkembang, membuat suatu paradigma bahwa tidak ada komputer yang aman kecuali dipendam dalam tanah sedalam 100 meter dan tidak memiliki hubungan apapun juga⁴. David Logic⁵

⁴ Sto, Seni Internet *Hacking*

berpendapat tentang Internet yang diibaratkan kehidupan jaman *cowboy* tanpa kepastian hukum di Amerika, yaitu:

"The Internet is a new frontier. Just like the Wild, Wild West, the Internet frontier is wide open to both exploitation and exploration. There are no sheriffs on the Information Superhighway. No one is there to protect you or to lock-up virtual desperados and bandits. This lack of supervision and enforcement leaves users to watch out for themselves and for each other. A loose standard called "netiquette" has developed but it is still very different from the standards found in "real life". Unfortunately, cyberspace remains wide open to faceless, nameless con artists that can carry out all sorts of mischief "

Seperti seorang *hacker*⁶ dapat masuk ke dalam suatu sistem jaringan perbankan untuk mencuri informasi nasabah yang terdapat di dalam server mengenai *data base* rekening bank tersebut, karena dengan adanya *e-banking* jaringan tersebut dapat dikatakan terbuka serta dapat diakses oleh siapa saja. Walaupun pencurian data yang dilakukan sering tidak dapat dibuktikan secara kasat mata karena tidak ada data yang hilang tetapi

⁵ David Logic, *Cybercrime* (California : 2004)

⁶ *Hacker* adalah seseorang yang dapat memasuki sistem jaringan komputer orang lain tanpa ijin

dapat diketahui telah diakses secara *illegal* dari sistem yang dijalankan.

Tidak kurang menghebohkannya adalah beredarnya gambar-gambar porno hubungan seksual/pornografi, misalnya antara seorang bintang sinetron Sukma Ayu dan Bjah, penyanyi yang sedang naik daun. Gambar-gambar tersebut beredar secara luas di Internet baik melalui *e-mail* maupun dalam tampilan *website* yang dapat disaksikan oleh siapa saja secara bebas⁷.

Pengungkapan kejahatan ini masih sangat kecil sekali, dikarenakan banyak kendala dan hambatan yang dihadapi dalam upaya pengungkapannya. Saat ini, bagi mereka yang senang akan perjudian dapat juga melakukannya dari rumah atau kantor hanya dengan mengakses situs www.indobetonline.com atau www.tebaknomor.com dan banyak lagi situs sejenis yang menyediakan fasilitas tersebut dan memanfaatkan fasilitas *Internet banking* untuk pembayarannya.

E-commerce tidak sedikit membuka peluang bagi terjadinya tindak pidana penipuan, seperti yang dilakukan oleh sekelompok pemuda di Medan yang memasang iklan di salah satu *website* terkenal "Yahoo" dengan seolah-olah menjual mobil

mewah Ferrary dan Lamborghini dengan harga murah sehingga menarik minat seorang pembeli dari Kuwait⁸. Perbuatan tersebut dapat dilakukan tanpa adanya hubungan terlebih dahulu antara penjual dan pembeli, padahal biasanya untuk kasus penipuan terdapat hubungan antara korban atau tersangka.

Dunia perbankan melalui Internet (*e-banking*) Indonesia, dikejutkan oleh ulah seseorang bernama Steven Haryanto⁹, seorang *hacker* dan jurnalis pada majalah Master Web. Lelaki asal Bandung ini dengan sengaja membuat situs asli tapi palsu layanan *Internet banking* Bank Central Asia, (BCA). Steven membeli domain-domain dengan nama mirip www.klikbca.com (situs asli Internet banking BCA), yaitu domain wwwklik-bca.com, kilkbca.com, klikbca.com, klickca.com, dan klikbac.com. Isi situs-situs plesetan inipun nyaris sama, kecuali tidak adanya security untuk bertransaksi dan adanya formulir akses (*login form*) palsu.

Jika nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkat situs plesetan yang dibuat oleh Steven sehingga identitas pengguna (*user id*) dan nomor identitas personal

⁷ Gatra, 20 Februari 2004

⁸ Waspada, 21 Februari 2005 dengan judul "Penipuan melalui Internet"

⁹ CyberTECH, 6 November 2002 dengan judul "Steven Haryanto"

(PIN) dapat di ketahuinya. Diperkirakan, 130 nasabah BCA tercuri datanya. Menurut pengakuan Steven pada situs bagi para *webmaster* di Indonesia, www.webmaster.or.id, tujuan membuat situs plesetan adalah agar publik menjadi lebih berhati - hati dan tidak ceroboh saat melakukan pengetikan alamat situs (*typo site*), bukan untuk mengeruk keuntungan.

Menurut perusahaan *Security Clear Commerce* di Texas USA, saat ini Indonesia menduduki peringkat ke 2 setelah Ukraina dalam hal kejahatan *Carding*¹⁰ dengan memanfaatkan teknologi informasi (Internet) yaitu menggunakan nomor kartu kredit orang lain untuk melakukan pemesanan barang secara *online*. Komunikasi awalnya dibangun melalui *e-mail* untuk menanyakan kondisi barang dan melakukan transaksi. Setelah terjadi kesepakatan, pelaku memberikan nomor kartu kreditnya dan penjual mengirimkan barangnya, cara ini relatif aman bagi pelaku karena penjual biasanya membutuhkan 3 – 5 hari untuk melakukan kliring atau pencairan dana sehingga pada saat penjual mengetahui bahwa nomor kartu kredit tersebut bukan milik pelaku barang sudah terlanjur terkirim.

¹⁰ Gatra , 13 September 2003

Selain *carding*, masih banyak lagi kejahatan yang memanfaatkan Internet. Tentunya masih hangat dalam pikiran kita saat seorang *hacker* bernama Dani Hermansyah, pada tanggal 17 April 2004 melakukan *deface*¹¹ dengan mengubah nama - nama partai yang ada dengan nama- nama buah dalam website www.kpu.go.id, yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap Pemilu yang sedang berlangsung pada saat itu.

Dikhawatirkan, selain nama – nama partai yang diubah bukan tidak mungkin angka-angka jumlah pemilih yang masuk di sana menjadi tidak aman dan dapat diubah, padahal dana yang dikeluarkan untuk sistem teknologi informasi yang digunakan oleh KPU sangat besar sekali. Untung sekali bahwa apa yang dilakukan oleh Dani tersebut tidak dilakukan dengan motif politik, melainkan hanya sekedar menguji suatu sistem keamanan yang biasa dilakukan oleh kalangan *underground*¹² (istilah bagi dunia *Hacker*). Terbukti setelah melakukan hal tersebut, Dani memberitahukan apa yang telah dilakukannya kepada *hacker* lain

¹¹ *Deface* adalah perubahan pada tampilan ataupun penambahan materi pada suatu *website* yang dilakukan oleh *hacker*.

¹² *Underground* adalah istilah yang sering digunakan oleh *hacker* untuk komunitasnya.

melalui *chat room* IRC khusus *Hacker* sehingga akhirnya tertangkap oleh penyidik dari Polda Metro Jaya yang telah melakukan *monitoring* di *chat room* tersebut¹³.

Deface disini berarti mengubah atau mengganti tampilan suatu *website*. Pada umumnya, *deface* menggunakan teknik *Structured Query Language (SQL) Injection*. Teknik ini dianggap sebagai teknik tantangan utama bagi seorang *hacker* untuk menembus jaringan karena setiap jaringan mempunyai sistem keamanan yang berbeda-beda serta menunjukkan sejauh mana kemampuan operator jaringan, sehingga apabila seorang *hacker* dapat masuk ke dalam jaringan tersebut dapat dikatakan kemampuan *hacker* lebih tinggi dari operator jaringan yang dimasuki.

Kelemahan *admin* dari suatu *website* juga terjadi pada penyerangan terhadap *website* www.golkar.or.id milik Partai Golkar. Serangan terjadi hingga 1577 kali melalui jalan yang sama tanpa adanya upaya menutup celah tersebut disamping kemampuan *Hacker* yang lebih tinggi, dalam hal ini teknik yang digunakan oleh *Hacker* adalah ***PHP Injection*** dan mengganti tampilan muka *website* dengan gambar wanita sexy serta gorilla putih sedang tersenyum.

¹³ Suara Merdeka , 27 April 2004 dengan judul "Polisi tangkap *Hacker* KPU"

Teknik lain adalah yang memanfaatkan celah sistem keamanan server alias *hole Cross Server Scripting (XXS)* yang ada pada suatu situs. *XXS* adalah kelemahan aplikasi di server yang memungkinkan *user* atau pengguna menyisipkan baris-baris perintah lainnya. Biasanya perintah yang disisipkan adalah *Javascript* sebagai jebakan, sehingga pembuat *hole* bisa mendapatkan informasi data pengunjung lain yang berinteraksi di situs tersebut. Makin terkenal sebuah *website* yang mereka *deface*, makin tinggi rasa kebanggaan yang didapat. Teknik ini pulalah yang menjadi andalan saat terjadi *cyberwar* antara *hacker* Indonesia dan *hacker* Malaysia, yakni perang di dunia maya yang identik dengan perusakan *website* pihak lawan¹⁴.

Menurut Deris Setiawan¹⁵, terjadinya serangan ataupun penyusupan ke suatu jaringan komputer biasanya disebabkan karena administrator (orang yang mengurus jaringan) seringkali terlambat melakukan *patching security* (instalasi program perbaikan yang berkaitan dengan keamanan suatu sistem). Hal ini mungkin saja disebabkan karena

¹⁴ Sinar Harapan , 10 April 2005 dengan judul "Cyber War Indonesia – Malaysia agar dihentikan"

¹⁵ Deris Setiawan, Sistem Keamanan Komputer, (Jakarta: PT Elex Media Komputindo, 2005)

banyaknya komputer atau server yang harus ditanganinya.

Dengan demikian maka terlihat bahwa kejahatan ini tidak mengenal batas wilayah (*borderless*) serta waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. Semua aksi itu dapat dilakukan hanya dari depan komputer yang memiliki akses Internet tanpa takut diketahui oleh orang lain/ saksi mata, sehingga kejahatan ini termasuk dalam *Transnational Crime*/ kejahatan antar negara yang pengungkapannya sering melibatkan penegak hukum lebih dari satu negara.

Mencermati hal tersebut dapatlah disepakati bahwa kejahatan IT/ *Cybercrime* **memiliki karakter yang berbeda dengan tindak pidana umum** baik dari segi pelaku, korban, modus operandi dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar KUHP.

Perkembangan teknologi informasi yang demikian pesatnya haruslah diantisipasi dengan hukum yang mengaturnya dimana kepolisian merupakan lembaga aparat penegak hukum yang memegang peranan penting didalam penegakan hukum, sebab tanpa adanya hukum yang mengatur dan lembaga yang menegakkan maka dapat menimbulkan kekacauan didalam

perkembangannya. Dampak negatif tersebut menimbulkan suatu kejahatan yang dikenal dengan nama **"CYBERCRIME"** yang tentunya harus diantisipasi dan ditanggulangi. Dalam hal ini Polri sebagai aparat penegak hukum telah menyiapkan unit khusus untuk menangani kejahatan *cyber* ini yaitu **UNIT V IT/CYBERCRIME** Direktorat II Ekonomi Khusus Bareskrim Polri.

PENGERTIAN CYBERCRIME

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*".

Andi Hamzah dalam bukunya "Aspek-aspek Pidana di Bidang Komputer" (1989) mengartikan *cybercrime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Sedangkan

menurut **Eoghan Casey**¹⁶ "Cybercrime is used throughout this text to refer to any crime that involves **computer and networks**, including crimes that do not rely heavily on computer". Ia mengategorikan cybercrime dalam 4 kategori yaitu:

1. *A computer can be the object of Crime.*
2. *A computer can be a subject of crime.*
3. *The computer can be used as the tool for conducting or planning a crime.*
4. *The symbol of the computer itself can be used to intimidate or deceive.*

Polri dalam hal ini unit cybercrime menggunakan parameter berdasarkan dokumen kongres PBB tentang *The Prevention of Crime and The Treatment of Offlenderes di Havana, Cuba* pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal :

- a. *Cyber crime in a narrow sense (dalam arti sempit) disebut computer crime: any illegal behaviour directed by means of electronic operation that target the security of computer system*

¹⁶ Eoghan Casey , *Digital Evidence and Komputer Crime*, (London : A Harcourt Science and Technology Company, 2001) page 16

and the data processed by them.

- b. *Cyber crime in a broader sense (dalam arti luas) disebut computer related crime: any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network.*

Dari beberapa pengertian di atas, cybercrime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/ alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

MODUS OPERANDI

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada¹⁷, antara lain:

a. Unauthorized Access to Computer System and Service

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu

¹⁷ Hinca IP Panjaitan dkk, *Membangun Cyber Law Indonesia yang demokratis* (Jakarta : IMLPC, 2005)

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

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

b. Illegal Contents

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

c. Data Forgery

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

d. Cyber Espionage

Merupakan kejahatan yang memanfaatkan jaringan Internet

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

e. Cyber Sabotage and Extortion

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

f. Offense against Intellectual Property

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Sebagai contoh, peniruan tampilan pada *web page* suatu situs milik

orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

g. Infringements of Privacy

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

UNDANG – UNDANG YANG DIKENAKAN

Menjawab tuntutan dan tantangan komunikasi global lewat Internet, Undang-Undang yang diharapkan (*ius constituendum*) adalah perangkat hukum yang akomodatif terhadap perkembangan serta antisipatif terhadap permasalahan, termasuk dampak negatif penyalahgunaan Internet dengan berbagai motivasi yang dapat menimbulkan korban-korban seperti kerugian materi dan non materi.

Saat ini, Indonesia belum memiliki Undang - Undang khusus/ *cyber law* yang mengatur mengenai *cybercrime* walaupun rancangan

undang undang tersebut sudah ada sejak tahun 2000 dan revisi terakhir dari rancangan undang-undang tindak pidana di bidang teknologi informasi sejak tahun 2004 sudah dikirimkan ke Sekretariat Negara RI oleh Departemen Komunikasi dan Informasi serta dikirimkan ke DPR namun dikembalikan kembali ke Departemen Komunikasi dan Informasi untuk diperbaiki. Tetapi, terdapat beberapa hukum positif lain yang berlaku umum dan dapat dikenakan bagi para pelaku *cybercrime* terutama untuk kasus-kasus yang menggunakan komputer sebagai sarana, antara lain:

a. Kitab Undang Undang Hukum Pidana

Dalam upaya menangani kasus-kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal - pasal yang dapat dikenakan dalam KUHP pada *cybercrime* antara lain :

1) Pasal 362 KUHP yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang

diambil dengan menggunakan *software card generator* di Internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.

2) Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

3) Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena

- pelaku biasanya mengetahui rahasia korban.
- 4) Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan *e-mail* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan *e-mail* ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.
 - 5) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di Internet dengan penyelenggara dari Indonesia.
 - 6) Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal.
 - 7) Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet , misalnya kasus Sukma Ayu-Bjah.
 - 8) Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.
 - 9) Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

b. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta.

Menurut Pasal 1 angka (8) Undang-Undang No 19 Tahun 2002 tentang Hak Cipta, **program komputer** adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak cipta untuk program komputer berlaku selama 50 tahun (Pasal 30).

Harga program komputer/ *software* yang sangat mahal bagi warga

negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual *software* bajakan dengan harga yang sangat murah. Misalnya, program anti virus seharga \$ 50 dapat dibeli dengan harga Rp20.000,00. Penjualan dengan harga sangat murah dibandingkan dengan *software* asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 perkeping.

Maraknya pembajakan *software* di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa **dengan sengaja dan tanpa hak memperbanyak penggunaan** untuk kepentingan komersial suatu program komputer dipidana dengan pidana penjara paling lama **5 (lima) tahun** dan/ atau denda paling banyak **Rp500.000.000,00 (lima ratus juta rupiah)**".

c. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 angka (1) Undang-Undang No 36 Tahun 1999,

Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik.

Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang-Undang ini, terutama bagi para *hacker* yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

- a) Akses ke jaringan telekomunikasi
- b) Akses ke jasa telekomunikasi
- c) Akses ke jaringan telekomunikasi khusus

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi "Barang siapa yang melanggar ketentuan sebagaimana

dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)”

d. Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan

Dengan dikeluarkannya Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya *Compact Disk - Read Only Memory* (CD - ROM), dan *Write - Once - Read - Many* (WORM), yang diatur dalam Pasal 12 Undang-Undang tersebut sebagai alat bukti yang sah.

e. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-Undang ini merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai

tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang (Pasal 2 Ayat (1) Huruf q).

Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Perbankan.

Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan.

Dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan

memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data-data tersebut.

Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau *digital evidence* sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

f. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Selain Undang-Undang No. 25 Tahun 2003, Undang-Undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

Digital evidence atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya

dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah *e-mail* dan *chat room* selain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin board* atau *mailing list*.

PENYIDIKAN TINDAK PIDANA

Menurut Undang-Undang No 2 Tahun 2002 tentang Kepolisian Pasal 1 angka 13 **penyidikan** adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam Undang-Undang untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya.

Dalam memulai penyidikan tindak pidana Polri menggunakan parameter alat bukti yang sah sesuai dengan Pasal 184 KUHP yang dikaitkan dengan segi tiga pembuktian/*evidence triangle* untuk memenuhi aspek legalitas dan aspek legitimasi untuk membuktikan tindak pidana yang terjadi. Adapun rangkaian kegiatan penyidik dalam melakukan penyidikan adalah

Penyelidikan, Penindakan, pemeriksaan dan penyelesaian berkas perkara.

1. Penyelidikan

Tahap penyelidikan merupakan tahap pertama yang dilakukan oleh penyidik dalam melakukan penyelidikan tindak pidana serta **tahap tersulit dalam proses penyidikan** mengapa demikian? Karena dalam tahap ini penyidik harus dapat membuktikan tindak pidana yang terjadi serta bagaimana dan sebab - sebab tindak pidana tersebut untuk dapat menentukan bentuk laporan polisi yang akan dibuat. Informasi biasanya didapat dari NCB/Interpol yang menerima surat pemberitahuan atau laporan dari negara lain yang kemudian diteruskan ke Unit *cybercrime*/ satuan yang ditunjuk.

Dalam penyelidikan kasus-kasus *cybercrime* yang modusnya seperti kasus *carding* metode yang digunakan hampir sama dengan penyelidikan dalam menangani kejahatan narkoba terutama dalam ***undercover*** dan ***control delivery***. Petugas setelah menerima informasi atau laporan dari Interpol atau *merchant* yang dirugikan melakukan koordinasi dengan pihak *shipping* untuk melakukan pengiriman barang.

Permasalahan yang ada dalam kasus seperti ini adalah laporan yang

masuk terjadi setelah pembayaran barang ternyata ditolak oleh bank dan barang sudah diterima oleh pelaku, disamping adanya kerjasama antara *carder* dengan karyawan *shipping* sehingga apabila polisi melakukan koordinasi informasi tersebut akan bocor dan pelaku tidak dapat ditangkap sebab identitas yang biasanya dicantumkan adalah palsu.

Untuk kasus *hacking* atau memasuki jaringan komputer orang lain secara ilegal dan melakukan modifikasi (*deface*), penyidikannya dihadapkan problematika yang rumit, terutama dalam hal pembuktian. Banyak saksi maupun tersangka yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit, belum lagi kendala masalah bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode digital yang membutuhkan SDM serta peralatan komputer forensik yang baik.

Dalam hal kasus-kasus lain seperti situs porno maupun perjudian para pelaku melakukan *hosting*/ pendaftaran diluar negeri yang memiliki **yuridiksi yang berbeda** dengan negara kita sebab pornografi secara umum dan perjudian bukanlah suatu kejahatan di Amerika dan Eropa walaupun alamat yang digunakan berbahasa

Indonesia dan operator daripada *website* ada di Indonesia sehingga kita tidak dapat melakukan tindakan apapun terhadap mereka sebab *website* tersebut bersifat universal dan dapat di akses dimana saja.

Banyak rumor beredar yang menginformasikan adanya penjabolan bank-bank swasta secara *online* oleh *hacker* tetapi **korban menutup-nutupi permasalahan** tersebut. Hal ini berkaitan dengan kredibilitas bank bersangkutan yang takut apabila kasus ini tersebar akan merusak kepercayaan terhadap bank tersebut oleh masyarakat. Dalam hal ini penyidik tidak dapat bertindak lebih jauh sebab untuk mengetahui arah serangan harus memeriksa server dari bank yang bersangkutan, bagaimana kita akan melakukan pemeriksaan jika kejadian tersebut disangkal oleh bank.

2. Penindakan

Penindakan kasus *cybercrime* sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali kita tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada

saksi yang mengetahui secara langsung.

Hasil pelacakan paling jauh hanya dapat menemukan IP *Address* dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana.

Penyitaan barang bukti banyak menemui permasalahan karena biasanya pelapor **sangat lambat dalam melakukan pelaporan**, hal tersebut membuat data serangan di *log server* sudah dihapus biasanya terjadi pada kasus *deface*, sehingga penyidik menemui kesulitan dalam mencari log statistik yang terdapat di dalam server sebab biasanya secara otomatis server menghapus log yang ada untuk mengurangi beban server. Hal ini membuat penyidik tidak menemukan data yang dibutuhkan untuk dijadikan barang bukti sedangkan data log statistik merupakan salah satu bukti vital dalam kasus *hacking* untuk menentukan arah datangnya serangan.

3. Pemeriksaan

Penerapan pasal-pasal yang dikenakan dalam kasus *cybercrime* merupakan suatu permasalahan besar yang sangat merisaukan, misalnya apabila ada *hacker* yang melakukan pencurian data apakah dapat ia dikenakan Pasal 362 KUHP? Pasal tersebut mengharuskan ada sebagian atau seluruhnya milik orang lain yang hilang, sedangkan data yang dicuri oleh *hacker* tersebut sama sekali tidak berubah. Hal tersebut baru diketahui biasanya setelah selang waktu yang cukup lama karena ada orang yang mengetahui rahasia perusahaan atau menggunakan data tersebut untuk kepentingan pribadi.

Pemeriksaan terhadap saksi dan korban banyak mengalami hambatan, hal ini disebabkan karena **pada saat kejahatan berlangsung atau dilakukan tidak ada satupun saksi yang melihat (testimonium de auditu)**. Mereka hanya mengetahui setelah kejadian berlangsung karena menerima dampak dari serangan yang dilancarkan tersebut seperti tampilan yang berubah maupun tidak berfungsinya program yang ada, hal ini terjadi untuk kasus-kasus *hacking*.

Untuk kasus *carding*, permasalahan yang ada adalah saksi korban kebanyakan berada di luar negeri

sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksaan untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban. Apakah mungkin nantinya hasil BAP dari luar negeri yang dibuat oleh kepolisian setempat dapat dijadikan kelengkapan isi berkas perkara? Mungkin apabila tanda tangan digital (*digital signature*) sudah disahkan maka pemeriksaan dapat dilakukan dari jarak jauh dengan melalui *e-mail* atau *messenger*.

Internet sebagai sarana untuk melakukan penghinaan dan pelecehan sangatlah efektif sekali untuk "pembunuhan karakter". Penyebaran gambar porno atau *e-mail* yang mendiskreditkan seseorang sangatlah sering sekali terjadi. Permasalahan yang ada adalah, mereka yang menjadi **korban jarang sekali mau menjadi saksi** karena berbagai alasan. Apabila hanya berupa tulisan atau foto2 yang tidak terlalu vulgar penyidik tidak dapat bersikap aktif dengan langsung menangani kasus tersebut melainkan harus menunggu laporan dari mereka yang merasa dirugikan karena kasus tersebut merupakan delik aduan (pencemaran nama baik dan perbuatan tidak menyenangkan).

Peranan saksi ahli sangatlah besar sekali dalam memberikan

keterangan pada kasus *cybercrime*, sebab apa yang terjadi didunia maya **membutuhkan ketrampilan dan keahlian yang spesifik**. Saksi ahli dalam kasus *cybercrime* dapat melibatkan lebih dari satu orang saksi ahli sesuai dengan permasalahan yang dihadapi, misalnya dalam kasus *deface*, disamping saksi ahli yang menguasai desain grafis juga dibutuhkan saksi ahli yang memahami masalah jaringan serta saksi ahli yang menguasai program.

4. Penyelesaian berkas perkara

Setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara maka permasalahan yang ada adalah masalah barang bukti karena **belum samanya persepsi diantara aparat penegak hukum**, barang bukti digital adalah barang bukti dalam kasus *cybercrime* yang belum memiliki rumusan yang jelas dalam penentuannya sebab *digital evidence* tidak selalu dalam bentuk fisik yang nyata.

Misalnya untuk kasus pembunuhan sebuah pisau merupakan barang bukti utama dalam melakukan pembunuhan sedangkan dalam kasus *cybercrime* barang bukti utamanya adalah komputer tetapi komputer tersebut hanya merupakan fisiknya saja sedangkan yang utama adalah data di dalam

hard disk komputer tersebut yang berbentuk file, yang apabila dibuat nyata dengan *print* membutuhkan banyak kertas untuk menuangkannya, apakah dapat nantinya barang bukti tersebut dalam bentuk *compact disc* saja, hingga saat ini belum ada Undang-Undang yang mengatur mengenai bentuk dari pada barang bukti digital (*digital evidence*) apabila dihadirkan sebagai barang bukti di persidangan.

UPAYA YANG DILAKUKAN

Untuk meningkatkan penanganan kejahatan *cyber* yang semakin hari semakin berkembang seiring dengan kemajuan teknologi maka Polri melakukan beberapa tindakan, yaitu:

a. Personil

Terbatasnya sumber daya manusia merupakan suatu masalah yang tidak dapat diabaikan, untuk itu Polri mengirimkan anggotanya untuk mengikuti berbagai macam kursus di negara-negara maju agar dapat diterapkan dan diaplikasikan di Indonesia, antara lain: CETS di Canada, Internet Investigator di Hongkong, Virtual Undercover di Washington, Computer Forensic di Jepang.

b. Sarana Prasarana

Perkembangan teknologi yang cepat juga tidak dapat dihindari sehingga Polri berusaha semaksimal mungkin untuk meng-*up date* dan *up grade* sarana dan prasarana yang dimiliki, antara lain Encase Versi 4, CETS, COFE, GSM Interceptor, GI 2.

c. Kerjasama dan koordinasi

Melakukan kerjasama dalam melakukan penyidikan kasus kejahatan *cyber* karena sifatnya yang *borderless* dan tidak mengenal batas wilayah, sehingga kerjasama dan koordinasi dengan aparat penegak hukum negara lain merupakan hal yang sangat penting untuk dilakukan.

d. Sosialisasi dan Pelatihan

Memberikan sosialisasi mengenai kejahatan *cyber* dan cara penanganannya kepada satuan di kewilayahan (Polda) serta pelatihan dan ceramah kepada aparat penegak hukum lain (jaksa dan hakim) mengenai *cybercrime* agar memiliki kesamaan persepsi dan pengertian yang sama dalam melakukan penanganan terhadap kejahatan *cyber* terutama dalam pembuktian dan alat bukti yang digunakan.