MERESPONS *fenomena* CYBERCRIME DI INDONESIA

Oleh : Drs. Agung Abdul Rasul, MM*

A. PENDAHULUAN

Sejalan dengan kemajuan teknologi informatika yang demikian pesat, melahirkan internet sebagai sebuah fenomena dalam kehidupan masyarakat Indonesia. Istilah fenomena sengaja diketengahkan karena Indonesia bukanlah negara pencipta bagi kemajuan teknologi informatika. Sebuah istilah yang memiliki implikasi yang berbeda bagi negara penemunya, karena bagi penemunya orientasi dan pemetaan tujuan pengembangan tehnologi informatika (TI) bukan hanya sekedar fenomena-melainkan merupakan sebuah *planning*.

Internet yang didefinisikan oleh **The US Supreme Court** sebagai *International Network of Interconnected Computer* merupakan kultur baru masyarakat modern. Dikatakan sebagai kultur, karena melalui internet berbagai aktifitas masyarakat *cyber (netizen)* seperti, berpikir, berkreasi dan bertindak sebagian dapat diekspresikan di dalamnya, kapanpun dan di manapun.

Kehadiran internet telah membentuk dunia tersendiri, yang dikenal dengan dunia maya (*cyberspace*) atau alam virtual (semu). Menurut **Roni Nitibaskara** disebut dunia karena pada kenyataannya *web-site interconnection* atau sistim dalam jaringan kompleks tehnologi informasi telah menjadi sub-sistim besar tersendiri, yang merupakan miniatur dunia. Komunitas masyarakat yang menghimpun diri dalam dunia maya ini semakin hari semakin meningkat.

Kecendrungan positif masyarakat untuk berkonsentrasi dalam *cyberspace* merupakan bukti bahwa internet telah membawa kemudahan-kemudahan bagi masyarakat bukan hanya sekedar sebagai sarana berkomunikasi, tetapi juga untuk memenuhi kebutuhan yang bersifat fisik, seperti melakukan transaksi bisnis tanpa harus melakukan interaksi secara fisik dan oleh karenanya dapat menembus batas geografis.

*) Redaktur Jurnal Studi Kepolisian

Komunitas Indonesia yang terhimpun dalam *cyberspace*, menurut hasil riset **Onno W. Purba** pada akhir tahun 2001, teridentifikasi sekitar 49.000 komunitas yang berpangkalan di *Yahoogroups.com*. Kuantitas ini oleh **Onno W. Purba** disinyalir sebagai kekuatan komunitas yang sangat besar yang terkonsentrasi di *cyberspace*.

Dari 49.000 komunitas tersebut, 2,4 % di antaranya atau 1170 komunitas berkembang dengan anggota lebih dari 100 orang, dan beberapa di antaranya mempunyai massa lebih dari 8000 orang. Secara rata-rata setiap komunitas memiliki anggota sekitar 364 orang. Masing-masing komunitas membentuk forum mulai dari forum silaturrahmi, keilmuan, bisnis, pornografi, religius, hobi hingga politik. Dari indikasi pesan yang berseliweran, hanya 2,9% yang merupakan pesan pornografi, dan partisipasi pesan/bulan/orang kurang dari 1 %, walaupun komposisi keanggotaan dalam komunitas pornografi ini mencapai 14,1 %. Namun demikian komposisi keanggotaan komunitas pornografi berada di atas porsentase forum religius, hobi dan politik.

Indikator tersebut relatif dapat menunjukkan bahwa netizen Indonesia memiliki karakteristik yang bisa menampik sisi gelap proses cybernation, khususnya *cyberporn*. Padahal Gambar porno sebagai sisi gelap dari cyberspace menurut **Neil Barett** mencapai 80 % dari seluruh gambar di internet. Di samping itu, menurut **American Demographics Magazine** yang diperoleh dari *sextracker.com* bahwa jumlah situs dewasa yang menyediakan pornografi melonjak 10 kali lipat pada tahun 2000 dibandingkan pada tahun 1997, atau meningkat dari 22.100 menjadi 280.300. **(Rapin Mudiardjo,e-mail rapin@ictwatch.com).**

Terlepas dari fenomena netizen Indonesia yang berpangkalan di *Yohoogroup.com*, fakta lain menunjukkan bahwa pada bulan Maret tahun 2000, Agus Wenas Setiawan, remaja 16 tahun asal Malang Jawa Timur semasa sekolah di Auastralia berhasil melakukan penyusupan ke dalam sistim informasi komputer data *storage Institute National Singapore University (DSINSU)*. Akibat perbuatannya, jaringan komputer milik perguruan tinggi negara itu tidak mampu memberikan pelayanan seperti sedia kala. Sebagian data-data penting rusak, sebagiannya lagi lenyap. Kerugian yang timbul ditaksir sebesar 15.505 Dollar Singapura. **(Roni NitiBaskara, 2001, hal.48).**

Di samping itu menurut **Indra Safitri** (www.Safitri.com.) bahwa sekelompok Hacker dari Rusia mencoba untuk memasuki jaringan

komputer elektronik milik Citibank. Perampokan elekronik itu bermaksud untuk membobol sebanyak $10 Juta, namun dapat digagalkan,tapi $ 400 ribu lenyap

Kemudian pada tahun 2002 menurut Mabes Polri telah terjadi 166 kasus cybercrime di Indonesia. 95,78 % di antaranya merupakan kejahatan yang difasilitasi oleh teknologi informasi, dan 4,22 % berupa kejahatan dengan sasaran sistim dan fasilitas "tehnologi informasi" (TI). Dari jenis kejahatan yang difasilitasi oleh TI, salah satu modus operandinya adalah *Credit Card Fraud* (pembobolan kartu kredit), dan menimbulkan kerugian lebih dari US $ 1,2 Juta atau di atas Rp 11,6 Milyar. Kupasan lebih detail sehubungan dengan *cybercrime* di Indonesia tahun 2002 dapat dilihat pada pembahasan selanjutnya.

Fakta-fakta di atas menunjukkan bahwa di Indonesia sisi positif dari kecanggihan *cyberspace* berbarengan pula dengan sisi negatif yang ditimbulkannya. Perkembangan *cyberspace*–yang telah demikian mengglobal– ternyata tidak selamanya menghasilkan hal-hal yang positif. Salah satu sisi negatifnya adalah tumbuh dan berkembangnya kejahatan di dunia cyber atau *cybercrime*..

Tulisan ini bermaksud untuk merespon sisi gelap dari *cyberspace*. Suatu bentuk respon yang banyak bersentuhan dengan uraian atas bentuk-bentuk *cybercrime* di Indonesia tahun 2002, dan kemudian ditawarkan beberapa scenario solusi berdasarkan hasil survei literatur

B. PENGERTIAN *CYBERCRIME* DAN PERKEMBANGAN *CYBERSPACE*

Cybercrime diidentikkan dengan kejahatan dari dunia maya (*cyberspace*) yang berbasis pada *computer network system* yang telah menjadi bagian dari *global operational system*, karena kemajuan tehnologi komputer dengan pirantinya ini pada gilirannya memang membentuk suatu tatanan dunia baru. Sebagai suatu dunia baru, dengan sendirinya membuka peluang bagi munculnya jenis-jenis kejahatan baru, atau *crime in cyberspace*, dengan meninggalkan pola dan bentuk-bentuk kejahatan konvensional dalam dunia nyata.

Kejahatan ini diawali dari sikap iseng dan anti kemapanan dari sejumlah kecil *hacker*, yang melakukan aksi-aksi illegal membobol sistim dan jaringan komputer yang ada. Dalam buku **The New Hacker Dictionary**, *Hacker* disebut sebagai programmer yang sangat ahli dan pintar. *Hacker* yang suka membobol sistim secara illegal disebut *Cracker*. Yang suka menyabot jaringan telepon

disebut *Phreaker*, sedang yang suka membobol kartu kredit disebut *Carder*, dan masih banyak lagi istilah lain yang melekat dengan tindakan *Cracker*.

Dalam beberapa literature, *cybercrime* sering diasosiasikan dengan *computer crime*. **The US Departemen Of Justice** memberikan pengertian *computer crime* sebagai... *any illegal act requiring knowledge of computer technologi for its perpetration, inverstigation, or prosecution*. Definisi tersebut menekankan substansi *cybercrime* pada tindakan kejahatan orang pintar pada teknologi komputer. Kemudian **Organizatation of European Community Development** menjelaskan bahwa tindakan kejahatan tersebut berupa perilaku tidak etis atau perilaku tanpa hak berkaitan dengan proses atau transmisi data. *Cybercrime is any illegal, unethical or unauthorized behaviour relating to the automatic processing and or the transmission data.*

Dalam perspektif yang lain, Ari **Juliana Gema** (WWW.theiceli.com) memberi batasan *cybercrime* dari sudut karakternya. Menurutnya karakter yang khas dari *cybercrime* antara lain ;

1. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi di ruang atau wilayah maya, sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan peralatan apapun yang bisa terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian material ataupun immaterial (waktu, nilai, jasa, uang,barang,harga diri, martabat, kerahasiaan informasi) yang cendrung 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.

Sementara itu **Roni Nitibaskara** (2001,hal.45) menjelaskan ciri-ciri khusus *cybercrime* sebagai berikut ;

1. *Non-violence* (tanpa kekerasan)
2. Sedikit melibatkan kontak fisik (*minimize of physical contact*)
3. Menggunakan peralatan (*equipment*) dan teknologi.
4. Memanfaatkan jaringan telematika (*telekomunikasi dan informatika*).

Cybercrime memiliki korelasi positif dengan perkembangan *cyberspace* yang dijembatani oleh perkembangan internet. Menurut

harian **Bisnis Indonesia** dalam **Ari Juliano Gema** (WWW.theiceli.com/dokumen/jurnal/ajo/a002.shtml-53k) bahwa saat ini internet sedang memasuki generasi ke II, yang mana dalam beberapa aspek berbeda dengan generasi ke I. Internet generasi I dapat diakses di atas meja, sarananya hanya PC, sumber pelayanannya *storefront web*, terjadi persaingan yang ketat antara *provider*, lingkup aplikasinya terbatas dan menempatkan TI sebagai asset. Sedangkan internet generasui ke II dapat diakses di mana saja, dengan menggunakan sarana apapun yang dapat terhubung dengan internet, sumber pelayannya *e-service otomatic*, antara *provider* terjadi hubungan transaksional, lingkup aplikasinya *e-service modular* dan memposisikan TI sebagai jasa.

Ari Juliano Gema juga mencirikan perbedaan karakteristik tindak kejahatan pada internet generasi I dan generasi ke II, terutama dari aspek Locus dan lingkup regulasi. Kalau pada internet generasi I locus tindak kejahatan selain masih terjadi pada satu sistim komputer, LAN atau WAN, juga di internet dan regulasinya masih berlingkup local. Sedangkan pada internet generasi ke II tindak kejahatan cendrung hanya terjadi di internet, dan sangat membutuhkan regulasi global.

Uraian di atas telah menunjukkan bahwa perkembangan *cyberspace* yang dijembatani oleh kemajuan teknologi informasi, berimplikasi pada munculnya *cybercrime* yang lebih kompleks.

C. MODUS OPERANDI *CYBERCRIME* DI INDONESIA TAHUN 2002

Berdasarkan data **Clear Commerce** pada tahun 2002 Indonesia berada di urutan kedua setelah Ukraina sebagai negara asal *Carder* terbesar di dunia. Sebelumnya pada tahun 2001 Survei **AC Nielsen** mencatat, Indonesia berada pada posisi keenam terbesar di dunia atau keempat di Asia dalam *cybercrime*. Karena dianggap sebagai sarang teroris *cyberspace*, banyak alamat IP *(Internet protocol)* Indonesia yang sempat diblokir, sehingga orang Indonesia yang ingin berbelanja melalui internet tidak dipercaya lagi oleh pemilik-pemilik situs belanja online di luar negeri. (**Heru Sutadi** dalam www.sinarharapan.co.id.

Kemudian menurut versi Mabes Polri,selama tahun 2002 tercatat 166 kasus *cybercrime*, yang mana 95,78 % merupakan kejahatan yang difasilitasi oleh TI Sedangkan sisanya 4,22 % berupa kejahatan dengan sasaran sistim dan fasilitas TI.

Berkenaan dengan kejahatan yang difasilitasi oleh TI, para

tersangka menggunakan modus operandi sebagai berikut ;

1. *Credit Card Fraud*

Credit card fraud (pembobolan kartu kredit) sebanyak 152 kasus, atau sekitar 95,60 % dari total kejahatan yang difasilitasi oleh TI. Kuantitas tersangka yang melakukan kejahatan ini menempati urutan teratas, yakni sebanyak 220 tersangka dan diidentifikasi seluruhnya berlokasi di Indonesia. Mereka sebagian besar terkonsentasi di pulau Jawa yakni sebanyak 81,19 %. Tersangka yang berlokasi di Yogyakarta sebanyak 28,44 %, di Jawa Tengah 19,72 %, di Jawa Barat 16,36 %, Jakarta 10,91 % dan Jawa Timur 5,50 %.

Untuk tersangka di luar pulau Jawa, dengan proporsi 18,81 %, bertebaran di pulau Sumatera sebanyak 8,26 %, pulau Sulawesi dan Kalimantan masing-masing sebanyak 1,38 %, dan pulau-pulau lain di Indonesia sekitar 7,80 %.

Sementara itu, korban dari *Credit card fraud* tersebut seluruhnya berlokasi di manca negara, yang mana korban paling tinggi berlokasi di USA sebanyak 54,19 %. Menyusul Canada dan Spain masing-masing sebanyak 16,13 dan 7,1 %. Untuk korban yang berlokasi di Jerman dan Australia masing-masing 5,16 %. Kemudian korban yang berlokasi di Inggris, Denmark, Jepang dan Singapura rata-rata sekitar 1,94 %. Negara-negara seperti Perancis, Austria, dan Korea juga tidak luput dari lokasi korban *Credit card Fraud*, sekalipun kuantitasnya relatif sedikit,yakni masing-masing sekitar 0,64 %.

Urutan kuantitas lokasi korban kejahatan *credit card fraud* di atas, besar kemungkinan mencerminkan urutan peringkat pemakaian *credit card on line* dalam transaksi bisnis di masing-masing negara tersebut. Pernyataan ini sejalan dengan hasil survei yang dilakukan oleh **Office Strategic Crime Assessment (OSCA)** tahun 1997 mengenai *Computer Crime & Security Survive* terhadap 2000 perusahaan di Inggris. Hasil survei tersebut menunjukkan adanya korelasi langsung antara peningkatan ketergantungan kepada tehnologi komputer dan tingkat penyalahgunaan system tersebut.

2. *Banking offences*

Banking Offences (penipuan perbankan) selama tahun 2002 hanya berjumlah 4 kasus atau sekitar 2,52 % dari total *cibercrime* yang difasilitasi oleh TI. Berbeda dengan *Credit card fraud*, di mana tersangka yang melakukan kejahatan ini seluruhnya berlokasi di Manca negara, 2 orang berlokasi di USA dan yang berlokasi di Malaysia dan Australia masing-masing 1 orang. Sedangkan korban dari kejahatan jenis ini justru berlokasi di di Solo dan Yogyakarta masing-masing 1 orang dan di Jakarta 2 orang.

3. *E-mail threats*

Seperti halnya *Credit Card fraud, E-mail threats* (ancaman melalui E-mail) dilakukan oleh tersangka yang berlokasi di tanah air, masing-masing 1 orang di Bandung dan Yogyakarta. Sedangkan korbannya masing-masing berlokasi di Jerman dan Australia. Kuantitas *cybercrime* dengan modus operandi *E-mail threats* sekitar 1,26 % dari total kejahatan yang difasilitasi oleh TI.

4. *Terrorism*

Sekalipun hanya 1 kasus, cybercrime dengan modus *terrorism* dengan tersangka Imam Samudra-pelaku utama dalam kasus peledakan bom di bali 12 Oktober 2002 tidak hanya menggegerkan para *netizen*, tetapi juga menarik perhatian masyarakat dunia. Atas tindakan tersangka, korbannya antara lain warga negara Australia, UK, USA, Jepang, Korea dan lain-lain.

Seorang *Cyber terrorist* mempunyai tujuan lebih dari sekedar uang dan ketenaran. Mereka biasanya lebih terorganisir dan mempunyai sumber dana untuk melakukan aksi-aksi terror. Target dari aksi *cyber terrorist* biasanya adalah sarana-sarana umum di dunia maya (*online facility*). (www.cbn.net.id/cbnweb/newletter/2003-02/newsletter03.asp-36 k).

Selanjutnya modus operandi kejahatan dengan sasaran sistim dan fasilitas teknologi informasi dapat diuraikan sebagai berikut;

1. *Ddos Attact*

Tercatat 3 kasus *Ddos (distribute denial of service) Attact* selama tahun 2002 yang melibatkan 1 tersangka dari Jakarta dan 2 orang dari Bandung. Serangan dengan *Ddos* bertujuan untuk melumpuhkan target (*Hang,crash*) sehingga sebuah *server* (komputer) tidak dapat memberikan layanan. Akibat dari *Ddos attacks* mengakibatkan masing-masing 1 korban dari Jepang, Denmark dan Singapura. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan, maka target tidak dapat memberikan layanan apapun kepada konsumennya, hingga mengalami kerugian finansial.

2. *Cracking*

Cracking dilakukan oleh *Cracker*. *Cracker* dapat didefinisikan sebagai *Hacker* yang suka membobol sistim secara illegal. Kejahatan cyber dengan modus *cracking* ini tercatat 3 kasus, atau 42,86 % dari total kejahatan dengan sasaran sistim dan fasilitas tehnologi informasi. Tersangka yang melakukan kejahatan jenis ini 2 orang berlokasi di Jakarta dan 1 orang di Medan.

Sementara itu, 2 diantara korbannya berlokasi di Jakarta dan 1 korban berlokasi di Singapura.

3. *Phreaking*

Selama tahun 2002 hanya tercatat 1 kasus *Phreaking*, atau 14,28% dari total kejahatan dengan sasaran sistim dan fasilitas TI. Baik tersangka maupun korban dari kejahatan jenis ini, keduanya berlokasi di Jakarta. *Phreaking* dilakukan oleh seorang *Phreaker*, yakni seorang *hacker* yang suka menyabot jaringan telepon.

4. *Worm/Virus Attacks*

Kejahatan dengan penyebaran virus (Worm/virus attacks) hanya 1 kasus, dan diduga tersangkanya berlokasi di China. Lokasi korban Kejahatan jenis ini masing-masing di Jakarta dan Bandung. Seperti halnya di tempat lain, virus komputerpun menyebar di Indonesia. Pada awalnya, beberapa nama virus komputer seperti *Friday 13 th, The Trojan Horse, Michael Angelo, Mardi Bross*, dan lain-lain berkembang pesat.

Sesuai dengan sifatnya, serangan virus-virus itupun beraneka ragam. Ada yang merusak data file, membuat *hang*, atau masuk ke dalam jaringan data komputer. Umumnya penyebaran dilakukan dengan menggunakan *email*, dan seringkali orang yang sistim *emailnya* terkena virus tidak sadar akan hal itu. Kasus virus ini sebelumnya sudah cukup banyak seperti virus *Mellisa, I Love You dan SirCam*.

D. RESPON CYBERCRIME SUATU SAMPEL SKENARIO

Disadari oleh berbagai kalangan bahwa untuk merespon cybercrime dalam bentuk membangun program anti cybercrime di Indonesia masih merupakan wacana. Pada sesi ini akan disajikan beberapa pandangan yang dihimpun oleh penulis berdasarkan hasil survei literatur. Berbagai pandangan yang akan disajikan berikut ini mungkin bermanfaat bagi perbendaharaan rujukan dalam mempertimbangkan upaya penanggulangan kejahatan cyber di tanah air.

1. Menangkal dengan Menelusuri Jejak *Hackers*.

Salah satu cara untuk menelusuri jejak Hacker menurut **Safitri** adalah dari "Sidik Jari Digital." Belajar dari pengalaman virus ganas Melissa yang menggegerkan beberapa tahun silam, menurut detektif *cyber* **Richard Smith** dari Brookline,Massachussets, *Hacker* ternyata meninggalkan sidik jari 32 digit (GUID/*Globally unique ID)* yang bisa mengidentifikasi komputer penulis virus. Inilah yang memungkinkan pembuat Melissa terlacak.

GUID biasanya tertanam dalam wujud file code komputer pada program *Microsoft office*. Kode inilah yang dijadikan Smith bersama rekannya dari Swedia menjejak nama si Pembuat virus, yang jelas-jelas namanya sebagai **David L Smith** dan akhirnya tertangkap. Cara serupa juga diterapkan para detektif dalam menangkap pelaku pembuatan virus *I Love You.* Dengan GUID sebuah file membuktikan adanya 40 nama *Hacker* dari *AMA Computer College*, Filipina.

2. Pemolisian di dunia *Cyber* (*Cyberpolice*)

Substansi dari *cyberpolice* adalah mendorong profesionalisme polisi dalam menghadapi kejahatan dunia maya. Dalam kaitan ini, pengalaman Biro Penyelidik federal AS (FBI) patut dijadikan pelajaran. Sejak tahun 1998, FBI telah membentuk NIPC (*National Infrastuktur Protection and Computer Intrusion*). Mereka dibekali dengan CART *(Computer Analisys Respon Team*) yang mampu memecahkan sandi yang ditinggal Hacker. **Safitri** (www.safitri.com).

3. Mendorong pengesahan RUU tentang Informasi, Komunikasi dan Transaksi Elekronik (IKTE) oleh DPR.

Dalam Undang-Undang ini tampaknya kejahatan yang berkait dengan TI telah diantisipasi, seperti perebutan nama Domain, Hacking, Cracking, Carding bahkan Pornografi. Undang-undang ini juga mampu menjaring orang luar Indonesia yang melakukan kejahatan TI yang dirasakan di Indonesia. **Heru Sutadi** (www.sinarharapan.co.id).

4. Proses pembelajaran *Cyber law.*

Mengingat kompleksnya persoalan yang dihadapi untuk menyelesaikan kasus pelanggaran hukum yang dilakukan melalui peralatan cyber, maka *Cyber law* sudah harus diajarkan pada mahasiswa fakultas hukum di Indonesia, termasuk para aparat penegak hukum.

Bentuk-bentuk respon yang mungkin dilakukan menghadapi cybercrime di atas adalah sekelumit ide atau mungkin hanya sample kecil dalam populasi ide yang begitu luas, dan tentunya merupakan scenario yang patut dipertimbangkan.

DAFTAR PUSTAKA

Ari Juliani Gema. *Cybercrime, Sebuah Fenomena Di Dunia Maya.* www.theceli.com/dokumen/journal.

Anonim. *Teroris Dunia Maya (Bagian I)*. www.cbn.net.id/cbn-web/newsletter/2003-02.

Barett,Neil..1997. *Digital Crime, Policing The Cibernation*, Kogan Page Ltd, London.

Heru Sutadi. *Cybercrime, Apa Yang Bisa Diperbuat*. www.sinarharapan.co.id

Indra Safitri. *Menangkal Dengan menelusuri Jejaknya*. www.Safitri.com/artikel-pdf/insider-journal.

....., Kejahatan Komputer Di pasar Modal. www.Safitri.com/artikel-pdf/insider-journal.

Onno W. Purba.2003. *Filosofi Naif Kehidupan Dunia Cyber*. Penerbit Republika

Rapin Mudiardjo. *Hukum Positif Dapat Bekerja Dalam Meng-antisipasi Cyberporn* e-mail rapin@ictwatch.com

Roni Nitibaskara.2001. *Ketika Kejahatan Berdaulat Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi.* Penerbit Harapan Jakarta.