Cybercrime
KEJAHATAN MAYA, KERUGIAN NYATA

Oleh : Jend. Pol (P) Drs. Chaeruddin Ismail*

A. PENDAHULUAN

Beberapa tahun lalu, berita pembobolan bank cukup banyak menarik perhatian masyarakat di negeri kita. Kejahatan yang dilakukan dengan cara mentranfer uang dari suatu bank ke rekening seseorang di bank lain. *Paswoord* (kunci sandi) komputer yang digunakan oleh bank tersebut. Setelah proses tranfer – bisa lebih dari satu kali pemindahan – uang tunaipun langsung ditarik, lalu si pelaku menghilang tanpa jejak. Sementara pembukaan rekening, si pelaku menggunakan identitas palsu sehingga tak mudah dilacak dalam waktu singkat. Contoh lain adalah penipuan dengan menggunakan telpon seluler (ponsel) yang juga melatarbelakangi dan beberapa pelakunya telah ditangkap.

Memang, kejahatan ini dapat dianggap sebagai bayang-bayang peradaban, atau "*crime is the shadows of civilization*". Sebuah peradaban di era teknologi informasi yang demikian canggih, yang ditandai dengan semakin meluasnya penggunaan komputer dan jaringannya, atau "*Computer network*" yang dengan segala piranti lunaknya, memungkinkan semua orang berkomunikasi dan berinteraksi dengan cepat, luas, hemat, dan tanpa batas: kapan saja, dimana saja, dan siapa saja.

The Borderless world, dunia memang jadi tanpa batas, dan dapat diwadahi hanya dalam sebuah screen monitor pada komputer. Hanya dengan menggunakan perangkat komputer melalui modern ke internet, ditambah dengan aneka software yang ada, memungkinkan semua orang bisa masukdalam dunia cyber (Cyberpace) tanpa "restu" dari siapapun. Membuat kehadiran Dunia cyber – dunia Maya – menjadi suatu realitas yang tak terhindarkan, dimana di dalam dunia maya ini, banyak orang berkumpul, berkomunikasi, dan berbisnis dalam satu komunitas yang tidak dibatasi oleh letak geografis.

---

* Mantan Kepala Kepolisian Republik Indonesia (Kapolri).

Karena setiap orang dapat menjadi anggota Cyberspace.

Namun, sisi positif dari kecanggihan cyberspace ini, ternyata berbarengan pula dengan sisi negatif yang ditimbulkannya. Perkembangan Cyberspace – yang selama demikian mengglobal – ternyata tidak selamanya menghasilkan hal-hal yang positif. Salah satu sisi negatifnya, antara lain adalah tumbuh dan berkembangnya kejahatan di dunia cyber atau cybercrime. Hilangnya batas ruang dan waktu di Internet mengubah banyak hal. Seseorang cracker di Eropa Timur dapat masuk dengan mudah ke sebuah server di Pentagon. Atau, sebaliknya seseorang di Pentagon pun bisa melakukan "intervensi" masuk ke dalam jaringan sistem informasi suatu negara, atau lembaga-lembaga tertentu, baik pemerintah maupun swasta.

Jika anda pernah menyaksikan film *The Enemy of State*, maka di saat digambarkan dengan mudah bagaimana identitas seseorang di delete dan digantikan dengan identitas orang lain. Bahkan, kartu kredit seseorang pun bisa hangus batas waktu, atau saldo yang tak tertinggal sepeserpun. Dan banyak lagi contoh-contoh lainnya, betapa cybercrime sesungguhnya merupakan sebuah ancaman nyata dari dunia Maya. Sebuah dunia yang baru, peluang dan tantangan baru, sekaligus ancaman yang baru pula.

Perubahan besar memang tengah terjadi, dimana semua orang – positif maupun negatif – akan terkena pula dampak dari kemajuan teknologi dunia cyber (cyberspace) yang maha pesat. Termasuk juga membuka peluang tumbuh dan berkembangnya bentuk-bentuk kejahatan di dunia Cyber atau *Crime on the Cyberspace*. Baik itu dalam bentuk computer crime, crime on the net, dan sejenisnya, dan seterusnya, yang notebene perkembangannya kian hari kian canggih. Ada dimensi baru kejahatan atau new dimention Crime yang bertolak dari computer network system serta merambah kesegenap aspek kehidupan, terutama ekonomi. Jadi, bukan semata-mata kejahatan nyata dimensi baru seperti white collar Crime, money loundering, dan lain-lain, melainkan – sebagai suatu kelebihan lantaran ia melewati computer system yang notabene lebih sulit dilacak.

B. PENGERTIAN

Apa yang disebut cybercrime, tak lain adalah bentuk kejahatan dari dunia cyber (Cyberspace) yang berbasis pada Computer network system yang telah menjadi bagian dari global operation system, karena kemajuan teknologi komputer dengan

pirantinya ini pada gilirannya memang membentuk sebuah "tatanan dunia baru". Sebagai suatu dunia baru, dengan sendirinya membuka peluang pada munculnya jenis-jenis kejahatan baru, atau Crime in Cyberspace, dengan meninggalkan pola dan bentuk-bentuk kejahatan konvensional dalam dunia nyata.

Sungguhpun pada mulanya, kejahatan ini diawali dari sikap iseng dan anti kemapanan dari sejumlah kecil orang-orang pintar yang menjadi hacker, yang melakukan aksi-aksi ilegal membobol sistem dan jaringan komputer yang ada. Dalam buku The New Hackers Dictionary, Hacker memang disebut sebagai programer yang sangat ahli dan pintar. Hacker yang suka membobol sistem secara ilegal disebut Cracker. Yang suka menyabot jaringan telepon disebut phreaker, sedang yang suka membobol kartu kredit disebut carder. Dan masih banyak lagi istilah lainnya, kendati menurut Steven Levy, pengarang buku Hackers, Heroes of The Computer Revolution, tanpa para Hackers tak akan ada internet. Bahkan adanya Hacker inilah justru kehidupan dunia maya menjadi lebih berwarna kendati ujung-ujungnya adalah ilegal action yang mereka lakukan, dan melahirkan para pengikut kejahatan dalam cyberspace.

Berikut ini beberapa jenis kejahatan dari dunia ini antara lain adalah;

Pemalsuan (Counterfeiting). Dengan segala kecanggihannya, teknologi komputer telah menciptakan suatu revolusi dalam hal pemalsuan. Teknologi baru ini – dalam hal pemalsuan – tidak saja telah memperluas lingkup operasi pemalsuan, tetapi juga telah membuat semakin sulitnya aparat penegak hukum untuk mendeteksinya. Bahkan, trend yang telah diidentifikasi oleh aparat penegak hukum di Australia, misalnya, telah terjadi peningkatan yang lebih canggih. Antara lain, pemalsuan Identitas, dokumen, sertifikat, identifikasi dan juga pemilikan dan asal usul. Hebatnya lagi, dokumen-dokumen ini dipakai pula untuk melakukan berbagai kegiatan penipuan, dan desepsi seperti membuka rekening bank (untuk money laundering, penghindaran pajak, dan lain-lain). Memperoleh kredit, perjanjian sewa beli, pencucian mobil, surat kelahiran, Sim, dan lain-lain).

Pornografi dan Perdagangan Sex Keleluasaan dan kebebasan jaringan computer system pada Internet pada gilirannya juga menyebabkan pornografi merajalela. Bukan saja situs-situs porno berkembang biak – yang melibatkan anak-anak – melainkan juga perdagangan sex pun mulai marak. Di Indonesia sendiri, situs-situs porno – milik lokal dalam negeri – sangat

marak perkembangannya. Bahkan sebagian besar di antaranya bisa memasuki atau disurfing dan di download secara gratis. Lalu, distribusi pornografi – baik dalam bentuk gambar maupun teks – menjadi suatu yang bebas dan terbuka. Bahkan, ada banyak kasus-kasus potongan film dan gambar porno para selebritis tanah air yang menyebar begitu rupa di Internet. Beberapa figur terkenal pernah menjadi "korban" kejahatan dari dunia Maya. Ini belum lagi dalam bentuk manipulasi gambar dan foto para tokoh dan orang terkenal kita – yang notabene sulit dibendung. Malah, ada banyak peristiwa dan kasus dimana internet merupakan sumber pertama kehebohan terjadi. Semua diawali dari kehebohan di Internet.

Transnational Gambling/Judi Internet juga mempermudah terselenggaranya perjudian transnational. Disamping perjudian tersebut, sering terjadi penipuan, karena operator jadi suka menipu. Masalah ini sangat sulit dilacak karena akan menyangkut jurisdiksi kalau operator judi berada (di negara lain) pencarian bukti-bukti dan lain-lain.

Pencurian dan penggunaan account Internet milik orang lain. Salah satu kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan yang "dicuri" dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, "pencurian" account cukup menangkap "userid" dan "password" saja. Hanya informasi yang dicuri. Sementara itu orang yang kecurian tidak merasakan hilangnya "benda" yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Misalnya, account yang ada menjadi berubah dan berbeda karena dicuri.

Membajak situs web. Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang terkenal dengan istilah deface. Pembajakan ini dapat dilakukan dengan mengeksploitasi lubang keamanan.

Probing dan port scanning. Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah dengan cara melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan "port scanning" atau "probing" untuk melihat pelayanan apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya.

Kejahatan Dengan Penyebaran Virus. Seperti halnya di tempat lain, virus komputer pun 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 itu pun beraneka macam. Ada yang merusak data file, membuat hang, atau masuk ke dalam jaringan data komputer. Lalu, pada perkembangan berikutnya aneka macam virus lain pun bermunculan. Bahkan, meningkat masuk ke dalam jaringan Internet Computer System, yang pada umumnya penyebaran dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, I love you, dan SirCam. Dan asal tahu saja, tercatat ada ribuan virus yang kini tengah beredar secara global.

Lalu, ada pula yang disebut Dos attack, yakni serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga sebuah server (komputer) tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan; maka target tidak dapat memberikanlayanan. Serangan ini tidak melakukan pencurian, penyadapan, atau pemalsuan data. Akan tetapi dengan hilangnya layanan, maka target tidak dapat memberikan layanan apapun kepada konsumennya, sehingga mengalami kerugian finansial. Dapat dibayangkan, bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial.

Kejahatan yang berhubungan dengan nama domain. Namun domain diguankan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain sebagaimana pernah terjadi pada kasus mustika-ratu.com. Kejahatan lain yang berhubungan dengan nama domain adalah membuat "domain plesetan", yaitu domain yang mirip dengan nama domain orang lain sebagaimana pernah terjadi dalam kasus Klikbca.com beberapa waktu lalu.

C. PERKEMBANGAN KEJAHATAN PADA ERA EKONOMI BARU

Perkembangan Internet pada gilirannya juga membuka peluang bagi tumbuh dan berkembangnya tatanan sarana ekonomi baru. Komunitas

bisnis dalam jaringan Internet, secara serempat merasakan keunggulan bertransaksi langsung secara efektif. Sebuah produsen bisa berhadapan langsung dengan target konsumennya. Juga, sebaliknya bagi konsumen dapat melakukan aneka macam pilihan sekaligus melakukan transaksi. Lalu, interaksi antara sesama pebisnis jauh lebih cepat, tepat dan efisien dengan menggunakan internet. Komunitas E-bussines menjadi suatu ajang berkumpulnya masyarakat bisnis, atau bagi mereka yang berkepentingan. Kata E-Commerce pun menjadi popular di dunia cyberspace.

Namun kebersamaan dengan itu, dibalik interaksi dan transaksi bisnis itu pun sesungguhnya membuka peluang yang sama untuk melakukan tindakan kejahatan. Bahkan, terdapat adanya anggapan internet merupakan tempat yang paling ideal untuk para penipu. Tempat subur bagi tumbuhnya crime in Cyberspace. Sebab, dengan melalui internet akan sangat mudah untuk nampak legal dan bonafid. Sebagai contoh adalah kasus "European Union Bank", yang hanya melalui cyberspace, atau internet, lembaga keuangan ini berhasil meraup US$. 10 juta dari para nasabahnya. Bahkan tak hanya itu, Crime in cyberspace juga dapat menyerang information system dari pemerintah, lembaga keuangan, dunia bisnis dan industri maupun perorangan.

Komunitas pebisnis yang memanfaatkan keuangan internet ataupun computer system sebagai sarana bisnis mereka, pada gilirannya justru – lambat laun – menciptakan ketergantungan kepada Teknologi (dependence of technology) yang tak selamanya selalu aman. "Ketergantungan yang meningkat dari dunia bisnis kepada system komputer telah membuat mereka lebih rentan terhadap kejahatan komputer. Banyak perusahaan lebih cemas terhadap bahaya kejahatan komputer daripada penipuan dan pencurian". Demikian hasil salah satu hasil survey dari 2000 perusahaan di Inggris, demikianpun hasil dari "Office of Strategic Crime Assessment (OSCA) 1997 Computer Crime & Security Survey". Hasil Survey tersebut menunjukkan adanya korelasi langsung antara peningkatan ketergantungan kepada teknologi komputer dan tingkat penyalahgunaan system tersebut.

Persoalannya adalah, siapakah para pelaku kejahatan komputer itu? Masih dalam hasil survey diatas, maka para pelakunya dapat dikategorikan; pelaku Internal (90%) adalah mereka yang mempunyai akses legal kepada system komputer. Kemudian pelaku External (60%) adalah yang berasal dari luar organisasinya (penetrasi pada system komputer hacking = system intrusion). Dimana hasil survey ini juga senada dengan hasil survey di Inggris, USA dan Eropa).

Dari data-data di atas ini, maka bukan mustahil dimasa mendatang external Computer Attack justru akan lebih meningkat, bahkan bisa menerobos dan merusak infrastruktur informasi dari suatu negara. Atau, pada suatu lembaga keuangan dan perbankan. Sebagai misal, pada banking operation system.

Dari data-data di atas ini, maka bukan mustahil dimasa mendatang external Computer Attack justru akan lebih meningkat dan makin canggih. Bahkan kini, dengan adanya Internet banking servis, digital cash, Smart Cards dan Digital signature verfication techniques, yang justru membuat bank cenderung lebih mudah dijangkau secara elektronik oleh masyarakat. Hal ini tentunya juga membuka peluang besar untuk hadirnya external attack kepada system perbankan.

D. PEMOLISIAN DI DUNIA CYBER (CYBERPOLICE)

Apapun namanya, Cibercrime tentu saja adalah sebuah kejahatan. Kejahatan Dunia Maya, namun mempunyai akibat Nyata. Dan setiap kejahatan tentunya harus ditangani secara maksimal, khususnya oleh aparat hukum yang kontempoten menangani hal ini. Namun, tentu saja tidak sederhana mengingat pengumpulan alat bukti yang menyangkut kejahatan komputer tidaklah mudah karena kejahatan dunia maya ini sangat spesifik, dimana data dalam file komputer mudah diganti, dihapus, atau dikacaukan sendiri oleh si pelaku. Bahkan, kini Computer Forensius sedang berkembang pesat. Sementara, Cyberpayment technologies yang meliputi transfer dana ke seluruh penjuru dunia berjalan dengan kecepatan tinggi dan sulit dibuktikan, jika mereka – para pelakunya – menggunakan kode program dan menghapusnya sendiri. Membuat hampir tidak mungkin bagi penyidik untuk melacak transfer uang secara elektronik itu.

Adapun langkah pertama untuk menanggapi masalah computer attack kepada system bisnis adalah reporting, atau pelaporan oleh yang bersangkutan sebagai korban. Namun, dalam kenyataannya, ternyata sangat sedikit yang melaporkan (menurut laporan PBB pada tahun 1994 diperkirakan hanya 5% yang dilaporkan), karena yang bersangkutan tidak tahu, bahwa system komputernya sudah diserang, atau karena tidak mau diketahui masyarakat bahwa system komputernya sudah dipenetrasi, demi menjaga citra dan krebilitasnya.

Sementara itu, terdapat pula beberapa hambatan dalam memperoleh tactical criminal imelligence. Hambatan yang ditimbulkan oleh teknologi canggih ini sangat ber-

pengaruh dalam memperoleh tactical criminal intellegence yang diperlukan oleh aparat penegak hukum, yakni antara lain meliputi adanya:

Encryption/Sandi

Pada saat sekarang sejumlah software developers dari negara-negara Eropa dan Asia sedang memasarkan produk-produk Encryption yang canggih. Penggunaan teknologi Encryption belakangan ini banyak dilakukan oleh pelaku kejahatan di Australia. Karena itu, kata-kata atau angka-angka sandi sangat mempersulit penyidikan aparat penegak hukum.

Anonymous Digital Cash

Pada saat sekarang terdapat berbagai macam digital cash, yang menyangkut smart card dan software based system seperti Mondex, Digicash, Quicklink, Trans Card dan Visa Cash. Beberapa diantara system tersebut memungkinkan dilakukan transaksi finansial secara anonim. Transaksi anonim ini membuka peluang untuk money laundering dan kegiatan illegal lainnya, yang sangat sulit/hampir tak mungkin dilacak oleh penyidik.

Anonymous Remailers

Dengan mempergunakan sebuah electronic remailer, dapat dikirim pesan, tanpa diketahui identitas pengirim berita oleh penerima berita. Sejumlah Remailer juga menyediakan encryption service. Penerima berita bisa berkomunikasi dengan pengirim berita tanpa diketahui identitasnya. Anonymous Remailers memberi kesempatan orang berbuat kejahatan dan tetap merahasiakan identitas mereka. Diperkirakan, penggunaan anonymous remailers untuk melakukan kejahatan ini, akan meningkat dalam waktu singkat.

Dari uraian di atas, nyatanya memang tak mudah memberantas Cybercrime mengingat pelbagai kecanggihan yang dimiliki oleh kemajuan teknologis komputer, selalu memungkinkan, atau memberi peluang pada si pelaku kejahatan untuk melakukan berbagai praktek dan bentuk kejahatan secara maya di dunia cyber. Tentu akan ada banyak anonymous-anonymous bentuk lain yang muncul dan menghilang begitu saja. Sementara perangkat hukum dan undang-undang, serta aneka cara untuk mengatasi cybercrime belum lagi optimal, khususnya lagi di negara kita. Polri sebagai aparat penegak hukum dan selaku penyidik, tentulah akan berhadapan dengan kejahatan maya yang sesungguhnya membutuhkan kemampuan dan keterampilan tersendiri. Bukan saja pengetahuan di dunia jaringan computer dan internet, tapi juga pengendalian dan penyidikan yang membutuhkan sarana dan prasarana teknologi

computerized system yang mampu mendeteksi dan mengenali lebih dini adanya cybercrime. Kemudian juga perangkat aturan main sehingga kewenangan penyidikan, khususnya dalam kejahatan ekonomi – keuangan dan perbankan – dunia maya ini, yang notabene merupakan wilayah-wilayah tersendiri dan amat sensitif.

Pemolisian dunia cyber, atau Cyberpolice juga tentunya akan mengalami banyak hambatan dan kendala mengingat partisipasi "korban" dunia maya ini, cenderung masih sangat passif dan sedikit orang yang mau melaporkan dirinya sebagai "korban" cybercrime lantaran sulit diketahui, siapa dimana dan bagaimana sesungguhnya si pelaku kejahatan itu. Sebab, bukti-bukti penyidikan dalam kejahatan konvensional seperti TKP, tak pernah bisa ditemui dalam cybercrime. Karena itu, upaya-upaya Cyberpolice, tak bisa tidak harus lebih kreatif, offensif, dan handal mengingat pengembang-biakan cybercrime cenderung semakin pesat. Namun, tentu saja tak ada kejahatan yang tak bisa ditangani. Termasuk juga cybercrime. Tergantung pihak Polri sendiri, sejauhmana kesiapannya menghadapi kejahatan dunia maya ini. Ini tentunya merupakan ujian dan tantangan tersendiri bagi institusi ini.

E. PENUTUP

Melihat pertumbuhan dan perkembangannya, Crime in Cyberspace tentu akan terus berkembang dengan pesat di Asia – Pasific, bahkan juga di seluruh dunia. Karena itu pendidikan dan kerjasama nasional, regional dan internasional dan melalui peninjauan kembali dari update undang-undang dan Police producers mutlak diperlukan agar kita tidak ketinggalan dalam perkembangan teknologi komputer, utamanya dalam menangani cybercrime.

Dengan adanya pengembang-biakan Cybercrime tentu saja merupakan persoalan serius. Seperti juga judul tulisan ini, Cybercrime, Kejahatan Maya – Kerugian Nyata tentu saja perlu ditangani secara serius. Dengan hadirnya Cybercrime, maka harus pula dihadirkan cyber-police. Ini artinya, harus ada upaya upaya pemolisian dalam memberantas – minimal mencegah atau mengeliminasi – pengembang-biakan lebih lanjut. Misalnya, dengan membentuk unit penanganan apakah itu dalam bentuk Indonesia Cyber-crime Responses Team, Indonesia Computer Security, dan lain sebagai-nya, ataupun dalam bentuk upaya-upaya preventip seperti melakukan sertifikasi perangkat security, yang secara khusus dapat menangkal cybercrime, baik dapat digunakan secara individual, kelompok ataupun

lembaga-lembaga yang berkepentingan dengan cybercrime. Di luar negeri sendiri, berbagai penanganan telah banyak dilakukan. Di Amerika Serikat, misalnya, telah memiliki lembaga seperti Computer Crime dan Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Departement of Justice. Lalu, ada pula apa yang disebut National Infrastructure Protection Center (NIPC) merupakan sebuah institusi pemerintah Amerika Serikat yang menangani masalah yang berhubungan dengan infrastruktur. Sementara di Korea Selatan, telah berdiri pula Korea Information Security Agency yang bertugas untuk melakukan evaluasi perangkat keamanan komputer & Internet, khususnya yang digunakan oleh pemerintah.

Namun, seperti juga kejahatan di dunia nyata, tindakan pemolisian dalam menangani kejahatan dunia maya ini – yang jelas merugikan secara nyata – tentu saja harus serta merta melibatkan masyarakat. Tanpa partisipasi masyarakat, baik sebagai objek maupun subjek atas tumbuh dan menggejalanya cybercrime, tak mungkin dilakukan penangkalan atas meluasnya tindak kejahatan dunia maya ini. Untuk itu, Polri sebagai salah satu aparat hukum yang berwenang, perlu menyadari hal ini.

DAFTAR PUSTAKA

AKDENIZ, YAMAN; Sex on the Net; The dilemma of Policing Cyberspace, South Street Press-Garnet Publishing Ltd; Reading UK, 1999.

BURNHAM, BILL; How to invest in E.Commerce Stocks; Mc Growhill, New York, 1999.

CUSUMANO, Michael A & David B. Yoffie; Compeiting On Internet Time; Lesson from Net Scape and It's Battle With Microsoft; TDUCHSTONE – Rockefellce Cewre, New York, 1998.

LONG. Andrew C & Partner; Youre Guide to E-Commerce Low in Singapore; Drew & Naiper; Singapore; 2000.

MELIALA, Andrianus; Mengungkap Kejahatan Kerah Putih, Pustaka Sinar Harapan; Jakarta: Cetakan II, 1995.

NURFAIZI, Mayjen Pol; Megatrend Kriminalitas, Jakarta Citra, 1998.

SAMBEL, Roy; Santoso Hanny (Ed); Bisnis Maya Laba Nyata; Bunga Rampai Konsep Aplikasi dan Tip Managemen Ekonomi Baru, PT. Elex Media Komputindo, Jakarta, 2002.

SLEVIN, James; The Internet and Society, Polity Press; Combidge – UK, 2000.

BUDI RAHARDJO, BUDI; PPAU Mikroelektronika ITB, IDCERT – Indonesia Computer Emergency Response Team, 2001.