DAMPAK NEGATIF DUNIA MAYA DALAM BAGI PERKEMBANGAN TEKNOLOGI INFORMASI DI INDONESIA

Eni Irfiani

ABSTRACT

The need of using computers that are connected one with another in 1969 opens a path to global interaction between users through internet technology. Internet development also influences the development of information technology in Indonesia. Up to 4.2 million people of Indonesia have made use of the internet. On one hand, it is useful for users. On the other hand, it opens possibilities for cyber crimes. Yet Indonesia has not had any force of law governing cyber crimes.

Dengan adanya kebutuhan pemakai untuk meggunakan komputer yang saling terhubung satu dengan yang lain pada tahun 1969, telah membuka jalan bagi pengguna komputer dapat berinteraksi secara global dengan menggunakan teknologi internet. Perkembangan internet juga berpengaruh terhadap perkembangan teknologi informasi di Indonesia. Hampir 4,2 juta masyarakat Indonesia telah menggunakan internet. Apabila ditinjau dari penggunaannya sangat menguntungkan pemakai namun di sisi lain muncul dampak negatif yang dapat membuka sarana modus kejahatan dunia maya. Hukum di Indonesia yang mengatur dunia maya belum memiliki kekuatan hukum sehingga akan terus muncul bentuk kejahatan-kejahatan lain.

I. PENDAHULUAN

Perkembangan teknologi informasi yang demikian pesat dan canggih, dengan aneka ragam layanan (*services*), mulai dari informasi umum hingga bisnis secara *online* melalui media internet telah membawa serangkaian persoalan baru, dengan berbagai dimensinya. Mulai dari dimensi ideologi, sosio-kultural masyarakat, ekonomi dan politik hingga hukum.

Salah satu revolusi terbesar yang mengubah nasib jutaan manusia dan kehidupan modern dewasa ini adalah ditemukannya komputer, yang segera disusul oleh berkembang pesatnya teknologi informasi (TI). Komputer seolah-olah benda ajaib yang menjadi rujukan apa saja, dan menjadi alat penghubung jutaan mungkin milyaran umat manusia.

Industri perangkat keras (*hardware*) komputer yang bersifat masif telah menyebabkan harga komputer, khususnya jenis *personal computer* (PC) menjadi terjangkau oleh kalangan yang luas. Akibatnya penggunaan komputer bukan lagi monopoli perusahaan atau kantor-kantor pemerintah saja. Rumah tangga dan perorangan pun sudah memanfaatkan teknologi ini.

Manfaat komputer semakin besar ketika terjadi konvergensi antara teknologi komputer dengan teknologi informasi (TI) dan teknologi komunikasi. Revolusi terbesar dari konvergensi ini adalah dibukanya akses publik terhadap penggunaan internet pada tahun 1955. Sejak saat itu, internet telah mengubah wajah sebagian besar dunia.

Dampak revolusi tersebut, dunia terikat menjadi satu oleh sistem elektronik yang menyalurkan berita

dan data dengan kecepatan cahaya ke seluruh tempat di dunia ini. Hanya dalam bilangan detik dan menit, bermilyar data ditransmisikan dari seluruh penjuru dunia.

Revolusi informasi, yang merupakan gabungan antara ilmu pengetahuan dan teknologi telah mengubah sumber kekayaan menjadi tidak lagi berupa materi tetapi berupa informasi, pengetahuan yang diterapkan pada pekerjaan untuk menciptakan suatu nilai. Siapa yang menguasai informasi maka ia akan menguasai dunia.

Dunia komputer selalu identik dengan teknologi telekomunikasi dan informasi yang disebut internet (*interconnected network*) atau jaringan yang saling terhubung. Di banyak negara di seluruh dunia tidak terkecuali di Indonesia, mengenal teknologi ini.

Di kota-kota kecil atau bahkan di pedesaan, sejauh memiliki sarana listrik, telepon dan provider internet, serta komputer dan peralatannya, sudah ada warung internet atau warnet. Para pelajar SMU saat ini sudah tidak lagi gagap teknologi.

Internet membuka cakrawala informasi, pengetahuan dan apapun fakta serta data lain dari seluruh penjuru dunia pula. Karena itu, teknologinya disebut sebagai *virtual technologi* atau teknologi maya. Disebut demikian sebab seolah-olah nyata padahal tidak, sebaliknya disebut tidak nyata padahal nyata. Sedangkan ruang maya yang terhubung komputer dengan saluran penyedia jasa internet yang dapat diakses kapan saja, tidak mengenal batas ruang dan waktu, akses dapat dilakukan untuk transaksi jual beli barang, tukar informasi atau bahkan merusak suatu jaringan komputer yang digelar oleh siapapun, baik pemerintah maupun swasta disebut juga dengan dunia maya (*cyber space*).

Perkembangan internet telah melewati perjalanan yang cukup panjang, namun cukup singkat jika dibandingkan dengan sejarah perkembangan teknologi perangkat keras (*hardware*) komputer.

Salah satu agenda penting masyarakat dunia dalam era informasi ini antara lain ditandai dengan penggunaan internet yang semakin meluas dalam berbagai aktivitas sehari-hari. Hal ini terjadi bukan saja di negara-negara maju, tetapi juga di negara-negara berkembang, termasuk Indonesia. Situasi tersebut pada gilirannya telah meningkatkan nilai informasi sebagai komoditas ekonomi yang sangat penting dan menguntungkan.

II. PEMBAHASAN

2.1. Sejarah Internet

Sejarah internet dimulai kira-kira pada tahun 1969 ketika Departemen Pertahanan Amerika Serikat mengadakan riset mengenai komputer. Ketika itu muncul kebutuhan untuk bagaimana caranya agar sejumlah komputer dapat terhubung dalam satu jaringan, sehingga dapat dilakukan kontak antar data dan pengguna.

Program awal riset tersebut dikenal dengan nama Arpanet. Perkembangan riset tersebut menunjukkan gejala baik, sehingga akhirnya pada tahun 1970 sudah berhasil menghubungkan 10 komputer. Jaringan kecil antar komputer ini sudah dapat saling berkomunikasi satu dengan yang lainnya.

Kemudian pada tahun 1972, Roy Tomlinson berhasil menyempurnakan program e-mail (electronic mail) yang dirintis satu tahun sebelumnya untuk Arpanet. Program e-mail ini begitu mudah,

sehingga langsung menjadi populer. Pada tahun yang sama, icon @ juga diperkenalkan sebagai lambang penting yang menunjukkan kata tempat "at" atau "pada". Tetapi, penggunaan dan popularitasnya masih terbatas.

Sejak tahun 1973, jaringan komputer Arpanet mulai dikembangkan meluas ke luar Amerika Serikat. Komputer University College di London merupakan komputer pertama yang ada di luar Amerika yang menjadi anggota jaringan Arpanet. Pada tahun yang sama, dua orang ahli komputer, yakni Vinton Cerf dan Bob Kahn, mempresentasikan sebuah gagasan yang lebih besar, yang menjadi cikal bakal pemikiran internet. Ide ini dipresentasikan untuk pertama kalinya di Universitas Sussex.

Karena komputer yang membentuk jaringan semakin hari semakin banyak, maka dibutuhkan sebuah protokol resmi yang diakui oleh semua jaringan. Maka pada tahun 1982 dibentuk *Transmission Control Protocol* atau TCP dan *Internet Protocol* atau IP yang kini dikenal oleh semua pengguna internet.

Sementara itu, di Eropa muncul jaringan komputer tandingan yang dikenal dengan Eunet, yang menyediakan jasa jaringan komputer di negara-negara Belanda, Inggris, Denmark dan Swedia. Jaringan Eunet menyediakan jasa e-mail dan newsgroup Usenet. Tampaknya, meskipun Eropa ketinggalan dari Amerika dalam riset awal internet, mereka tetap tidak mau ketinggalan.

Untuk menyeragamkan alamat di jaringan komputer yang ada, maka pada tahun 1984 diperkenalkan sistem nama domain, yang hingga kini kita kenal dengan DNS atau *Domain Name System*. Komputer yang tersambung dengan jaringan sudah melebihi 1000 komputer. Setahun kemudian, alamat anggota jaringan mulai menggunakan akhiran .com (dotcom).

Sistem alamat yang praktis ini langsung menggelembungkan jumlah komputer yang tersambung di jaringan. Pada 1987, jumlah komputer yang tersambung ke jaringan melonjak hingga 10 kali lipat menjadi 10.000 lebih. Pada saat itu, agaknya sudah banyak pihak yang bukan hanya mulai memahami potensi internet untuk lebih dari sekedar sarana telekomunikasi, melainkan juga memanfaatkan potensi itu untuk masa depan bisnis dan komersial.

2.2. Perkembangan Internet di Indonesia

Saat ini diperkirakan terdapat 407,1 juta pengguna internet di seluruh dunia atau sekitar 6,72 persen dari total populasi dunia yang berjumlah sekitar enam milyar jiwa lebih. Demikian hasil perhitungan Global Internet Policy Initiative (GIPI) internews. Dari hasil penelitian ini, Indonesia hanya tercatat memiliki 400 ribu pengguna internet atau hanya 0,18 persen dari total penduduk yang lebih dari 225 juta jiwa.

Angka untuk Indonesia ini masih jauh di bawah perkiraan 4,2 juta pengguna internet yang dikeluarkan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada awal tahun 2002. Tidak jelas dari mana angka 400 ribu tersebut diperoleh. Mungkin data GIPI diperoleh dari rekaman (*record*) resmi, yang statistiknya jelas di bawah angka riil.

Jika menggunakan hasil penelitian GIPI itu, Indonesia terpuruk di posisi ke-47 pada jumlah pengguna internet.

Meskipun demikian, masyarakat Indonesia tidak perlu berkecil hati. Bisnis warnet (warung internet) telah merambah ke mana-mana. Di luar isu mengenai substansi

atau isi internet yang dimanfaatkan para pengguna *(users)* warnet, ketersediaan akses internet yang mulai meluas itu agak menggembirakan.

2.3. Dampak Perkembangan Internet

Dampak dari internet dan teknologi TI begitu besar. Hampir semua kantor saat ini sudah menggunakan media internet sebagai basis informasi. Bahkan bagi banyak kantor penggunaan internet begitu vital, sehingga apabila terjadi kemacetan di dalam akses tersebut dapat dipastikan aktivitas di dalam kantor itu akan terhenti.

Tetapi aktivitas kerja dengan menggunakan internet sangat gampang disalah gunakan. Menurut majalah *PC World*, di Amerika Serikat, satu dari lima perusahaan swasta disana telah mengambil tindakan disipliner terhadap para pegawai yang menyalahgunakan jaringan internet lewat komputer di kantor mereka.

Harian *The New York Times* menuliskan, sekitar 25 persen lalu-lintas internet lewat komputer di kantor tidak ada hubungannya dengan pekerjaan. Selain itu tercatat 37 persen pegawai yang di survei mengakui sering menggunakan jaringan internet yang tidak ada hubungannya dengan tugas-tugas mereka.

Hal itu menandakan betapa rentannya penggunaan internet dalam menunjang pekerjaan. Tetapi setidaknya memang segala perubahan itu membawa konsekuensi. Dalam kehidupan manusia, teknologi selalu membawa sisi yang baik dan juga sisi yang buruk. Sifat ini akan terus begitu hingga akhir jaman.

Di samping segala kemudahan yang ditimbulkan oleh perkembangan teknologi TI ternyata dunia maya juga memunculkan potensi kejahatan baru yang disebut kejahatan maya *(cyber crime)*.

Kejahatan komputer di dunia maya adalah kejahatan yang dilakukan oleh orang yang mahir dan paham menggunakan komputer dan internet. Saking pahamnya, orang yang bersangkutan bisa memanfaatkan kelemahan dan kelebihan komputer untuk suatu tindak kejahatan.

Orang-orang yang melakukan kejahatan maya tersebut umum dikenal sebagai *cracker* dan *hacker*. Seseorang yang melakukan tindakan kejahatan dengan memasuki serta menganggu hingga merusak sistem orang lain disebut sebagai *cracker*. Sedangkan tindakan seorang *hacker* tidak sampai merusak, yang dilakukan biasanya hanya sekedar mengintip informasi tentunya secara diam-diam, tanpa melakukan perubahan apapun terhadap sistem yang dia masuki. Tindakan tersebut dinamakan hacking.

Dari berbagai kasus yang terungkap dan pelakunya tertangkap, sebagian di antaranya terbukti bahwa kejahatan maya umumnya dilakukan oleh anak-anak muda, bahkan remaja. Di antara kasus-kasus besar kejahatan tersebut, ada di antaranya yang merupakan hasil dari sekedar tindakan iseng atau coba-coba.

Para ahli kemudian meramalkan, bahwa kejahatan ini akan menjadi kejahatan penting pada masa depan. Hal ini seiring dengan berkembangnya teknologi komputer.

Karena itu, sangat perlu untuk mengenali dan mendeteksi terus-menerus perkembangan teknologi yang memungkinkan terjadinya *cyber crime*. Lebih dari itu, dIperlukan keahlian dan ketrampilan yang memadai dari aparat penegak hukum –khususnya kepolisian- untuk menangani kasus-kasus *cyber crime*.

Tentu saja, polisi tidak mungkin mengatasi *cyber crime* secara sendirian. Tanpa kesadaran publik, khususnya para pengguna (*users*) komputer dan internet, sulit untuk kenghapus *cyber crime*. Karenanya harus ada upaya sosialisasi terus-menerus kepada *users*, khususnya para *crackers* dan *hackers*, bahwa tindakan mereka membawa konsekuensi hukum.

Demikian pula halnya dengan perangkat hukum yang mampu mencegah *cyber crime*. Undang-undang dan berbagai peraturan lain harus terus menerus di mutakhirkan (*update*) dan diperbaiki, guna mampu mengantisipasi *cyber crime*.

Dalam bidang hukum, perangkat yang ada di Indonesia sama sekali belum memadai, baik untuk pengaturan maupun kerangka pengendalian dan hukuman atas tindakan kejahatan maya. Perangkat hukum berupa Undang-Undang seharusnya berfungsi sebagai pencegah (*preventif*) kemungkinan terjadinya pertikaian karena memberikan kerangka aturan main.

2.4. Jenis-jenis *cyber crime*

Perkembangan teknologi informasi (TI) yang demikian cepat tidak hanya menciptakan berbagai keuntungan dan kemudahan bagi pengguna, tapi juga membuka sarana baru berbagai modus kejahatan. Ironisnya, dari hari ke hari, kejahatan maya kian meningkat, baik kuantitas maupun kualitasnya. Meski penetrasi TI masih rendah, nama Indonesia ternyata begitu populer dalam kejahatan di dunia maya ini.

Kejahatan komputer pada dunia maya muncul pertama kali di Amerika Serikat dan menghebohkan dunia pada tahun 1980an. Teroris *cyber crime* Kevin Mitnick, salah satu *hacker* paling terkenal di dunia. Ia menjadi begitu populer setelah berhasil menjebol jaringan dan mencuri software di perusahaan-perusahaan seperti Sun Microsystems dan Motorola. Dia bisa menemukan nomor jaminan keamanan mantan presiden AS, George Bush senior dan nama kecil ibunda Leonardo DiCaprio dalam waktu kurang dari 15 detik. Dan kemampuan seperti inilah yang membuatnya menjadi buruan FBI selama tiga tahun karena ia menyusup ke perusahan-perusahaan terbesar di dunia. Hobby itu akhirnya menjadikannya sebagai salah satu orang yang paling dicari FBI. Ketika akhirnya tertangkap, ia harus mendekam selama lima tahun di penjara AS tahun 1990-an.

Dari referensi yang ada di Indonesia menunjukkan bahwa munculnya *cyber crime* pertama kali di Indonesia tidak dapat ditelusuri kejadiaanya, kapan, dan kasus apa. Namun demikian dapat dikemukakan bahwa era 1990-an adalah era awal masuknya fenomena *cyber crime* di Indonesia. Di lihat dari putusan pengadilan bahwa kasus yang pertama kali disidangkan adalah kasus pemakaian domain mustika-ratu.com oleh perusahaan pesaing atau lebih dikenal dengan istilah *cyber squatting*. Pelakunya Tjandra Sugiono hanya dihukum 4 bulan penjara.

Secara garis besar *cyber crime* terdiri dari dua jenis, yaitu :

1. Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas.

Contoh-contoh dari aktivitas *cyber crime* jenis pertama ini adalah pembajakan (*copyright* atau hak cipta intelektual, dan lain-lain), pornografi, pemalsuan dan pencurian kartu kredit (*carding*), penipuan lewat e-mail, pembobolan rekening bank, perjudian online, terorisme, transaksi

obat terlarang, transaksi seks dan lain-lain.

2. kejahatan yang menjadikan sistem dan fasilitas teknologi informasi (TI) sebagai sasaran.

Cyber crime jenis ini bukan memanfaatkan komputer dan internet sebagai media atau sarana tindak kejahatan, melainkan justru menjadikannya sebagai sasaran. Contohnya adalah pengaksesan ke suatu sistem secara ilegal (*hacking*), perusakan situs internet dan server data (*cracking*) serta melakukan perubahan isi dari halaman situs (*defacting*).

2.5. Kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas

a. Pembajakan

Kejahatan ini berupa pembajakan atas hak cipta intelektual (Hak Atas Kekayaan Intelektual-HAKI) milik orang atau pihak lain. Pihak yang memiliki hak cipta dirugikan, karena karya mereka dibajak dan disebarluaskan tanpa pembelian atau pembayaran royalti.

b.Kasus Pornografi

Sebagian masyarakat menganggap hadirnya situs-situs porno bukanlah suatu kejahatan, sebaliknya masyarakat lain menganggap pornografi sebagai kejahatan. Meskipun kontroversial, pornografi di internet jelas merupakan tindakan kejahatan jika menyangkut eksploitasi anak-anak, pedofilia.

c. Pemalsuan dan Pencurian Kartu Kredit

Kasus ini di Indonesia biasa disebut carding. Aktivitas ini merupakan aktivitas ilegal yang banyak terjadi di Indonesia dan dilakukan oleh orang-orang yang secara sengaja mengambil informasi kartu kredit seseorang, seperti nama, alamat, nomor pin, nomor kartu kredit, password, dan lain-lain.

Dengan informasi itulah si pembobol informasi kartu kredit tadi melakukan transaksi pembelian melalui internet. Barang dipesan dengan kartu kredit yang dibobol itu, untuk dikirim ke si pembobol dengan alamat tertentu – boleh jadi alamatnya sendiri atau alamat transit (barang). Sedangkan tagihannya akan dikenakan kepada si empunya kartu kredit yang sesungguhnya.

Berdasarkan data *ClearCommerce* tahun 2003 lalu, Indonesia berada diurutan kedua setelah Ukraina sebagai negara asal *carder* (pembobol kartu kredit) terbesar di dunia.

Sebelumnya, survei AC Nielsen 2001 mencatat, Indonesia berada pada posisi keenam terbesar di dunia atau keempat di Asia dalam tindak kejahatan *cyber*. Karena dicap sebagai sarang teroris dunia maya, banyak alamat IP (*Internet Protocol*) Indonesia yang sempat diblokir. Sehingga, orang Indonesia yang ingin berbelanja lewat Internet tidak dipercaya lagi oleh pemilik-pemilik situs belanja online di luar negeri.

Sejauh ini, di dalam negeri, kasus penyadapan e-mail, PIN (*personal identification number*) untuk *internet banking*, pelanggaran hak *privacy*, pemalsuan nama *domain*, penggunaan kartu kredit milik orang, serta berbagai efek negatif lainnya sudah tidak terhitung jumlahnya. Data kejahatan yang difasilitasi TI periode Januari-September 2002 yang dikeluarkan Mabes Polri cukup mencengangkan. Karena, dari 104 kasus yang melibatkan 124 pelaku diketahui 98% di antaranya dari Indonesia. Sisanya dari Inggris, Malaysia, serta negara Asia lain.

d. Penipuan lewat e-mail

Modus ini beragam dan umumnya calon korban didapat dengan cara dikirimi e-mail. Isinya mulai dari sekedar ajakan untuk masuk ke suatu situs tertentu, hingga e-mail yang berisi ajakan kerjasama. Penyebaran informasinya juga dilakukan melalui iklan-iklan gratis yang bertebaran di internet.

e. Perjudian Online

Perjudian online merupakan kasus yang pelik. Bila praktek perjudian terjadi di suatu lokasi, agak mudah bagi kepolisian bila ingin menindaknya. Tidak demikian dengan perjudian lewat internet.

Dengan perangkat teknologi yang makin canggih, seorang penjudi tidak perlu bersusah payah untuk datang ke suatu arena perjudian. Tetapi dia cukup duduk di rumah dengan aman, menggunakan internet dan menggunakan fasilitas kartu kreditnya untuk melakukan aktivitas perjudian di dalam suatu situs.

Perjudian di internet tidak mengenal batas umur, wilayah dan status sosial seseorang. Olah karena itu tidak menutup kemungkinan seorang anak dapat menjelajahi website judi dan turut bermain dalam suatu taruhan. Terlebih lagi perjudian online dan para pemainnya melintasi batas-batas geografis dan lintas usia.

f. Pencurian dan Penggunaan *Account* Internet Milik Orang Lain

Salah satu kesulitan sebuah ISP (*Internet Service Provider*) adalah adanya account pelanggan yang mereka curi dan digunakan secara tidak sah. Sementara itu, orang yang kecurian tidak merasakan kehilangan, namun akibat dari pencurian account ini, pengguna dibebani biaya penggunaan *account* tersebut.

Akibat serius dari pencurian *account* adalah jika *account* tersebut dipakai dalam modus operansi *cyber crime* yang lain. Penjahat cyber yang menggunakan *account* orang lain lebih sulit di lacak.

g. Terorisme

Internet adalah salah satu sarana favorit para teroris dalam melakukan tindakan terorisme. Kegunaan minimal adalah sebagai sarana komunikasi, karena lebih sulit dilacak ketimbang melalui sarana telepon. Terlebih lagi jika para anggota jaringan teroris itu menggunakan sandi dan kode-kode lain dalam berkomunikasi.

Tindakan teroris lain yang menyangkut internet adalah pencurian data dan informasi melalui internet, dan penyerangan terhadap suatu sistem tertentu dari sarana strategis milik negara. Pusat kendali pertahanan Amerika Serikat, Pentagon, misalnya.

h. Isu SARA

Isu SARA digolongkan dalam *cyber crime*, karena aktivitas ini dipandang dari beberapa sudut bisa sangat berbahaya. Sebagai contoh sebuah situs yang isinya menyebarkan rasa kebencian terhadap Yahudi, Muslim dan Sikh Dharma Ontario di Amerika Serikat.

Memang jarang ditemukan situs yang secara terang-terangan menampilkan isu SARA. Tetapi biasanya kebencian tersebut disebarkan melalui milis (*mailing list*).

i. Situs Sesat

Kasus lain yang juga dimasukkan dalam *cyber crime* adalah situs sesat, seperti yang terjadi di Korea Selatan. Kepolisian Korea Selatan menyelidiki sebuah situs sesat yang isinya mengajak orang yang mengunjungi situs tersebut untuk melakukan bunuh diri.

2.6. Kejahatan yang menjadikan Sistem dan Fasilitas TI sebagai sasaran

a.Pencurian Data Pribadi

Pencurian data pribadi adalah trend kejahatan yang cepat sekali meluas. Karena aktivitas ini memang mudah dilakukan. Banyak sekali bertebaran software yang mudah dijalankan oleh seorang pemula sekalipun.

Dengan menambah ketrampilan dari sekedar mengintip (*hack*), seorang hacker bisa berubah menjadi cracker.

Kasus di New York pada tahun 2003 sebuah Toko Kinko, Juju Jiang memasang Invisible Keylogger Stealth dalam beberapa unit komputer di toko itu. Dan Jiang memanfaatkan informasi yang didapatnya dari aplikasi tersebut untuk tindak kejahatan, termasuk mengakses rekening bank dan rekening sistem pembayaran *online*.

b. Pembuatan dan Penyebaran Virus Komputer

Kasus ini merupakan jenis kasus yang sulit ditindak. Karena perkembangan program yang digolongkan sebagai virus komputer sangat cepat. Sekarang ini, perkembangan virus komputer baru muncul dalam hitungan setiap satu jam. Untuk melakukan *update* sebuah program dalam hitungan satu bulan sekali saja merepotkan, palagi kalau harus di-update dalam hitungan jam

c. Pembobolan Situs

Aktivitas pembobolan situs sangat berbahaya dan merugikan. Salah satu kasus yang paling menghebohkan di Indonesia ketika Pemilu 2004. Situs Komisi Pemilihan Umum (KPU) dibobol oleh *cracker*. Perolehan suara parpol yang dipresentasikan secara online oleh KPU tiba-tiba mengalami perubahan informasi secara mendadak. Nama-nama partai politik resmi diubah menjadi Partai Kelereng, Partai Jambu, Partai Cucok Rowo dan lain-lain.

Beberapa hari kemudian, aparat satuan *Cyber Crime* Direktorat Reserse Khusus Kepolisian Daerah Metro Jaya menangkap Dani Firmansyah (25), yang diduga kuat sebagai pelaku pembobol situs tersebut.

d. *Cyber War*

Perang di dunia cyber tampaknya semakin menjadi alternatif dari perang sesungguhnya. Keusilan, kenakalan, dan bahkan keahlian, *hacker* yang tersebar di seluruh dunia mendorong mereka berlaga di arena ini. Interpretasi nasionalisme semacam itu mendorong hacker mengerahkan kemampuannya untuk menerobos, melumpuhkan, dan menyerang pengguna komputer atau sistem keamanan negara lain.

Model baru peperangan lewat internet dalam bentuk aksi saling serang modern, yang tidak dibatasi jarak dan waktu, benar-benar terjadi. Model seperti ini dapat menyebabkan ketakutan yang luar biasa bagi perusahaan besar yang membawa bendera negara-negara yang bersengketa.

Ketakutan tersebut memang masuk akal, karena terkadangpara hacker tidak pandang bulu dalam melancarkan serangannya. Konflik di Timur Tengah yang tak kunjung usai, menimbulkan peperangan via internet tidak kunjung henti pula, terutama antara Israel dengan Palestina.

Begitu pula halnya ketika terjadi konflik antara India dengan Pakistan. Dalam kasus perang cyber ini, aksi para hacker Pakistan berhasil membobol situs-situs India. Estonia beberapa bulan baru ini mengumumkan bahwa negaranya telah menjadi target serangan *hacker*

Rusia. Walaupun secara resmi Rusia membantahnya namun bisa jadi serangan itu memang nyata. Jerman, Perancis dan Amerika diberitakan telah mendapatkan serangan bertubi-tubi dari China yang menginginkan informasi-informasi ekonomi, dan ilmu pengetahuan. Saat kisruh hubungan Indonesia dengan Malaysia, terjadi saling serang di dunia maya.

e. Membajak Situs *Web*

Salah satu kegiatan yang sering dilakukan *cracker* adalah mengubah halaman web, atau lebih dikenal dengan *deface*. Pembajakan halaman *web* dapat dilakukan dengan mengeksploitasi lubang keamanan. Menurut data statistik di Indonesia hingga April 2001 menunjukkan setidaknya satu situs *web* dibajak tiap hari.

f. *Denial of Service* (DoS) dan *Distributed Denial of Service* (DdoS) *Attack*

DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (*hang, crash*) sehingga sasaran serangan tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi, dengan hilangnya layanan, maka target tidak dapat memberikan layanan sehingga ada kerugian finansial.

g. Kejahatan yang berhubungan dengan Nama Domain

Nama domain (*domain name*) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang mencoba menarik keuntungan dengan mendaftarkan nama domain nama perusahaan orang lain, dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah *cyber squatting*. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain, seperti kasus mustika ratu.com.

Kejahatan lain yang berhubungan dengan nama domain adalah membuat 'domain plesetan', yaitu nama domain yang mirip dengan nama domain orang lain (seperti kasus klikbca.com). Istilah yang digunakan saat ini adalah typo-squatting. Setelah squatting, pelaku *cyber crime* dapat melakukan scam untuk menipu calon klien yang masuk ke dalam domain-nya.

2.7. Faktor-faktor yang Mempengaruhi Terjadinya *Cyber Crime*

a. Faktor politik

Penyebaran virus komputer dapat merusak jaringan komputer yang digunakan pemerintah, perbankan, pelaku usaha maupun perorangan. Dapat dipastikan apabila jaringan komputer perbankan tidak berfungsi dalam satu hari saja dapat menimbulkan kekacauan pembayaran maupun transaksi keuangan nasabah.

Kondisi ini memerlukan kebijakan politik pemerintah Indonesia untuk menanggulangi *cyber crime* yang berkembang di Indonesia. Aparat penegak hukum telah berupaya keras menindak setiap pelaku *cyber crime*, tapi penegakan hukum tidak dapat berjalan dengan maksimal sesuai harapan karena perangkat hukum yang mengatur khusus tentang *cyber crime* belum ada.

Untuk menghindari kerugian yang lebih besar akibat tindakan pelaku *cyber crime* maka diperlukan kebijakan politik pemerintah Indonesia untuk menyiapkan perangkat hukum khusus (*lex specialist*) bagi *cyber crime*. Dengan perangkat ini penegak hukum tidak ragu-ragu lagi dalam

melakukan penegakan hukum terhadap *cyber crime*.

b. Faktor Ekonomi

Jaringan komputer dan internet merupakan media yang sangat murah untuk melakukan promosi barang-barang produksi. Masyarakat dunia banyak memanfaatkan media ini untuk mencari barang-barang untuk kepentingan perusahaan ataupun perorangan.

Krisis ekonomi yang melanda suatu bangsa, menjadikan media ini untuk mencari keuntungan pribadi dengan mudah. Seorang hacker bisa menemukan tool-tool untuk melakukan *cyber crime* dengan mudah di internet.

c. Faktor Sosial Budaya

Teknologi sebagai hasil temuan dan pengembangan manusia dapat dimanfaatkan untuk perbaikan kemanusiaan, namun disisi lain dapat membawa petaka bagi manusia sebagai akibat adanya penyimpangan.

Diantara media internet sebagai wahana berkomunikasi, secara sosiologis terbentuklah sebuah komunitas para pecandu internet yang saling berkomunikasi, bertukar pikiran berdasarkan prinsip kebebasan dan keseimbangan diantara para pecandu atau maniak dunia maya tersebut.

Komunitas ini adalah sebuah populasi gaya baru sebagai gejala sosial, dan sangat strategis untuk diperhitungkan. Penyimpangan atas aktivitas dan kreativitas di bidang cyber tidak dapat dibendung lagi. Komunitas mereka terbentuk berdasarkan kepentingan emosional dan berbagai motivasi diantara para interner.

2.8. Upaya Pencegahan *Cyber Crime*

1. Pengenalan komputer pada masyarakat

   Sosialisasi komputer dan internet di tengah-tengah masyarakat, misalnya dalam dunia pendidikan, seminar teknologi informasi.

2. Peran serta masyarakat

   Dilibatkannya masyarakat dalam pencegahan kejahatan maya adalah untuk mengeliminir faktor-faktor kriminogen yang ada dalam masyarakat dan menggerakkan potensi masyarakat dalam hal mencegah dan mengurangi kejahatan.

2.9. Pengamanan Software Jaringan Komputer

a. Mengatur akses (*access control*) dengan menggunakan password.

b. Firewall, program yang merupakan sebuah perangkat yang diletakkan antara internet dengan jaringan internal, tujuannya adalah untuk menjaga agar akses ke dalam maupun ke luar dari orang yang tidak berwenang tidak dapat dilakukan.

c. Intruder Detection System (IDS), diantaranya adalah autobuse, mendeteksi probing dengan memonitor log file.

d. Back-up rutin

2.10. Faktor-Faktor yang Saling Berhubungan Dalam *Cyber Crime*

a. Pelaku Kejahatan

Pelaku mempunyai keunikan-keunikan tersendiri, yang belum tertampung dalam konsep-konsep atau teori konvensional.

b. Modus operandi kejahatan

Modus operandi *cyber crime* berbeda dari tindak kejahatan konvensional. Yang paling mencolok adalah locus delicti (tempat kejadian

perkara) karena sangat sulit melokalisir jaringan internet.

c. Korban kejahatan

Korban tidak selalu dalam bentuk yang dapat dilihat (*tangible*) melainkan juga yang tidak terlihat (*intangible*). Karena tempat tinggal dan kewarganegaraan korban yang tidak selalu sama dengan pelaku *cyber crime*, maka penegak hukum menghadapi masalah yang lebih kompleks.

d. Reaksi sosial atas tindakan kejahatan

Pada kejahatan konvensional, reaksi massa terhadap pencuri yang tertangkap berupa penghakiman massa. Sebaliknya reaksi masyarakat atas *cyber crime* tidak sebesar pada kejahatan konvensional.

e. Hukum

UU dan perangkap hukum serta aturan lain bersifat empiris. *Cyber crime* belum terumus secara jelas, dan perkembangan kerangka hukum yang ada kalah pesat dibandingkan dengan perkembangan kejahatan yang terjadi.

2.11. Ancaman terhadap Keamanan Informasi

Menurut *PC Magazine* edisi April 2007 terdapat 10 ancaman terhadap keamanan informasi yang sering terjadi:

a. *Social engineering*

Social engineering bisa juga diartikankan sebagai intelijen manusia. Sehingga ancaman keamanan informasi nomor satu adalah manusianya. Orang-orang yang bersentuhan dengan informasi penting dan rahasia tersebutlah yang berpotensi untuk membocorkannya. Potensi kebocoran informasi berada pada si pembuat, si pengguna, si pengolah, si pendistribusi dan atau si penyimpan informasi.

Kebocoran informasi akibat kegiatan sosial ini kadang disengaja untuk maksud tertentu, namun lebih sering tidak disengaja akibat orang tersebut terpancing dalam suatu pembicaraan atau kegiatan atau argumen tertentu atau *blackmail*.

b. *Identity theft*

Di kehidupan sehari-hari, tidak mungkin seseorang berjalan di muka umum dengan topeng wajah orang lain tanpa diketahui. Namun di dunia digital hal tersebut dapat dilakukan dengan mudah.

Identity theft atau pencurian informasi tentang identitas kita dapat dilakukan melalui komputer *off-line*, jaringan LAN dan internet maupun melalui transaksi-transaksi dikehidupan sehari-hari. Saat ini hipnotis dapat juga dimasukkan sebagai salah satu cara pencurian identitas.

Motif pencurian identitas biasanya adalah uang, namun tidak tertutup kemungkinan motif lain yang bersifat pribadi, politik ataupun bisnis.

c. *Spyware* dan *trojans*

Spyware dan *trojan horse* adalah program komputer yang biasanya tanpa sengaja terinstal untuk melakukan perusakan, penyalinan dan/atau pengintipan aktifitas sebuah komputer, sehingga segala aktifitas kita saat menggunakan komputer dapat dipantau, di-*copy* atau didalangi dari tempat lain.

Spyware dan *trojans* biasanya terinstal karena ketidak-telitian pengguna komputer saat meng-klik suatu *pop-up* atau *browsing* internet.

d. Virus dan *worm*

Virus dan *worm* adalah sebuah program komputer aktif yang biasanya tersembunyi dan membahayakan karena bersifat

merusak komputer. Virus dapat menginfeksi program komputer lain dan/atau *file* data serta dapat terdistribusi ke komputer lain dengan membonceng pendistribusian file/program lain.

e. *Adware*

Adware adalah kependekan dari *advertising software*, yaitu sebuah program yang dibuat untuk mengiklankan sesuatu yang dapat secara otomatis tampil dalam web *browser* atau *pop-up*. *Adware* bisa ter-*download* tanpa sengaja bila kita tidak teliti saat meng-klik iklan yang tampil dalam sebuah *pop-up*.

f. Web exploits

Terkadang kita mendapati sebuah *website* yang didalamnya berisi kode-kode jahat (*malicious codes*) yang dapat mengeksploitasi lubang-lubang keamanan dalam sistem operasi dan program yang digunakan dalam komputer kita.

Dengan hanya dengan mengunjugi situs tersebut, komputer kita dapat terinfeksi atau dirusak olehnya.

g. *Hacker attack*

Hacker adalah seseorang atau beberapa orang yang ahli dan mengetahui seluk beluk komputer baik software, hardware, keamanan atau jaringannya.

Hacker sering dikonotasikan sebagai penjahat di dunia komputer. Namun sesungguhnya tidak semua *hacker* melakukan kejahatan, terdapat pula *hacker* yang memang berfungsi sebagai peneliti dan pengembang dengan cara menelusuri lubang-lubang keamanan sebuah software atau jaringan komputer.

h. *Wireless attack*

Dengan kehadiran prosesor dan software sistem operasi terbaru, teknologi *wireless* telah mulai menjadi "barang biasa". *Wireless* sangat menguntungkan dari segi problem pemasangan kabel dan kabel yang semrawut. Namun bila tidak hati-hati, seseorang dalam jangkauan area *wireless* tersebut dapat "mencuri" *bandwidth* kita. Bahkan orang tak dikenal tersebut dapat menjelajahi komputer dalam jaringan *wireless* tersebut, sebab orang tak dikenal itu berada "didalam" jaringan.

i. *Phishing mail*

Phising mail adalah sebuah email yang seolah-olah dikirim dari bank tempat kita menyimpan uang, dari situs tempat kita membeli barang secara *on-line* dan lain-lain yang mirip-mirip seperti itu.

Bila kita *log-in* kedalam situs gadungan tersebut maka situs itu akan mencuri *username* dan *password* yang akan merugikan kita.

j. *Spam mail*

Spam mail atau *junk mail* atau *bulk mail* biasanya berupa e-mail yang dikirim secara serentak ke beberapa alamat yang berisi pesan penawaran, tipuan dan lain-lain yang biasanya kurang berguna bagi penerimanya.

2.12. Cara-cara Untuk Menghindari Ancaman Keamanan Informasi

a. Jangan gunakan program yang diberikan oleh orang yang tidak dikenal.
b. Bacalah peringatan keamanan yang muncul sebelum meng-klik-nya.
c. Gunakan *password* dengan benar.
d. Gunakan program firewall, antivirus, antispyware, antispam yang baik dan selalu diperbaharui.

e. *Back-up* file-file penting dalam sebuah media eksternal dan simpan ditempat yang aman.
f. Berhati-hatilah saat meng-klik sebuah situs yang dirujuk dalam sebuah e-mail.
g. Gunakan sistem penyandian yang baik untuk melakukan koneksi *wireless* ataupun menyimpan dan mendistribusikan data.

2.13. Upaya Antisipasi Kejahatan Maya Secara Hukum

Pada dasarnya setiap kegiatan atau aktifitas manusia dapat diatur oleh hukum. Hukum disini direduksi pengertiannya menjadi peraturan perundang-undangan yang dibuat oleh negara, begitu pula aktifitas kejahatan mayantara yang menjadikan internet sebagai sarana utamanya ini. Dalam kaitan dengan teknologi informasi khususnya dunia maya, peran hukum adalah melindungi pihak-pihak yang lemah terhadap eksploitasi dari pihak yang kuat atau berniat jahat, disamping itu hukum dapat pula mencegah dampak negatif dari ditemukannya suatu teknologi baru.

Akan tetapi pada kenyataannya hukum sendiri belum dapat mengatasi secara riil terhadap permasalahan-permasalahan yang ditimbulkan oleh teknologi khususnya teknologi informasi. Salah satu bukti kongkretnya adalah timbulnya berbagai kejahatan di dunia *cyber* yang ternyata belum bisa diatasi sepenuhnya oleh hukum.

Saat ini berbagai upaya telah dipersiapkan untuk memerangi *cyber crime*.

The Organization for Economic Co-operation and Development (OECD) telah membuat petunjuk bagi para pembuat kebijakan yang berhubungan dengan kejahatan yang berhubungan dengan komputer, dimana pada tahun 1986, OECD telah mempublikasikan laporannya yang berjudul "*computer related crime: analysis of legal policy*". Laporan ini berisi hasil survei terhadap peraturan perundang-undangan negara-negara anggota beserta rekomendasi perubahannya dalam menanggulangi kejahatan yang berhubungan dengan komputer tersebut, yang mana diakui bahwa sistem telekomunikasi juga memiliki peran penting didalam kejahatan tersebut. Melengkapi laporan OECD, The *Council of Europe* (CE) berinisiatif melakukan studi mengenai kejahatan tersebut.

Studi ini memberikan petunjuk lanjutan bagi para pengambil kebijakan untuk menentukan tindakan-tindakan apa yang seharusnya dilarang berdasakan hukum pidana negara-negara anggota dengan tetap mempehatikan keseimbangan antara hak-hak sipil warga negara dan kebutuhan untuk melakukan proteksi terhadap kejahatan yang berhubungan dengan komputer. Pada perkembangannya, CE membentuk Committee *of Experts on Crime ini Cyber space of The Committee on Crime Problem*, yang pada tanggal 25 April 2000 telah mempublikasikan *draft Convension on Cyber Crime* sebagai hasil kerjanya, yang menurut Prof. Susan Brenner dari University of Daytona School of Law, merupakan perjanjian internasional pertama yang mengatur hukum pidana dan aspek proseduralnya untuk berbagai tipe tindak pidana yang berkaitan erat dengan penggunaan komputer, jaringan atau data.

Instrument Hukum Internasional publik yang mengatur masalah kejahatan siber yang saat ini paling mendapat perhatian adalah konvensi tentang Kejahatan Siber (*Convention*

on Cyber Crime) 2001 yang digagas oleh Uni Eropa. Konvensi ini meskipun pada awalnya dibuat oleh organisasi regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan siber. Substansi konvensi mencakup area yang cukup luas, bahkan melindungi masyarakat dari cyber crime, baik melalui undang-undang maupun kerjasama internasional.

Di Indonesia sendiri, setidaknya sudah terdapat Rancangan Undang-Undang Informasi dan Transaksi Elektronik (RUU ITE) yang di gawangi oleh Direktorat Aplikasi Telematika Departemen Komunikasi dan Informatika. Subyek-subyek muatannya ialah menyangkut masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara *e-comerce*, azas persaingan usaha usaha tidak sehat dan perlindungan konsumen, azas-azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional serta azas *Cyber Crime*.

RUU tersebut mengkaji kasus-kasus kejahatan dunia maya dalam beberapa sudut pandang secara komprehensif dan spesifik, fokusnya adalah semua aktivitas yang dilakukan dalam dunia maya (*cyberspace*) untuk kemudian ditentukan pendekatan mana yang paling cocok untuk regulasi Hukum Cyber di Indonesia.

Sejak Maret 2003 lalu di Kantor Menteri Negara Komunikasi dan Informasi (Menkominfo), tengah digodok Rancangan Undang-Undang (RUU) Informasi dan Transaksi Elektronik (ITE)-yang semula bernama Informasi, Komunikasi dan Transaksi Elektronik (IKTE). Sebetulnya, RUU ITE merupakan informasi sejak 1997.

gabungan dari dua RUU, yaitu RUU tentang Pemanfaatan TI (PTI), dan Tandatangan Elektronik dan Transaksi Elektronik (TE). RUU PTI disusun oleh Ditjen Pos dan Telekomunikasi, Departemen Perhubungan, bekerja sama dengan Tim dari Fakultas Hukum Universitas Padjadjaran (Unpad) dan Tim asistensi dari ITB.

Sementara RUU TE dimotori Lembaga Kajian Hukum dan Teknologi Universitas Indonesia (UI) dengan jalur Departemen Perindustrian dan Perdagangan.

Menurut Profesor Dr. Mieke Komar, Ketua Tim perumusan RUU PTI Unpad, RUU yang dibuat bersama 10 anggota timnya itu seluruhnya terdiri atas 13 bab dan 42 pasal dan penjelasan. Selain mengatur kelembagaan, RUU ini juga mencakup aturan perdagangan elektronik, nama domain, dan perlindungan hak atas kekayaan intelektual (HaKI) dan perlindungan terhadap hak-hak pribadi. Sudah tentu RUU juga mencakup penyelesaian sengketa, yurisdiksi, dan kewenangan pengadilan, perpajakan, penyidikan, ketentuan pidana, dan aturan peralihan.

Menilik cakupan isinya yang luas, RUU ini tampaknya belum memasukkan semua aspek dari industri TI. Hal itu bisa dimengerti, karena RUU ini dimaksudkan menjadi payung bagi aturan-aturan yang ada di bawahnya. Jika semua aspek dimasukkan, bisa jadi justru membingungkan, sehingga pengimplementasiannya juga tidak optimal. Idealnya, pemerintah perlu membuat UU untuk setiap bagian khusus seperti digital signature, e-banking, e-Governmet, atau UU spesifik lainnya. Inilah dilakukan Malaysia yang sejak tahun 1997 telah memiliki perangkat hukum teknologi

Oleh karena itu Indonesia harus mau menunggu lebih lama lagi

karena sampai saat ini belum ada pegangan dalam bentuk UU lain.

Hal ini tidak mungkin dilakukan dalam kondisi seperti saat ini karena jika proses pembentukan *cyber law* terlalu lama, bisa jadi perkembangan TI di Indonesia sama sekali tidak membawa dampak positif, tapi justru hanya merugikan negara. Selain itu, jika UU dibuat secara terpisah-pisah juga berpotensi menimbulkan inkonsistensi dan kesulitan dalam penggabungan jika diperlukan, terutama menyangkut penyelesaian kasus yang berkaitan.

Yang menarik, RUU PTI juga mengatur perluasan masalah yurisdiksi yang memungkinkan pengadilan Indonesia mengadili siapa saja yang melakukan tindak pidana bidang TI yang dampaknya dirasakan di Indonesia. Contohnya, jika *cracker* asing melakukan kejahatan terhadap satu bank di Indonesia, maka berdasarkan pasal 33 dan 34 RUU PTI, pengadilan Indonesia berwenang mengadili orang itu jika masuk ke Indonesia. Selama ini kejahatan yang melibatkan orang Indonesia dan asing sangat marak, namun penyidikan kejahatan siber tersebut selalu terganjal yurisdiksi.

Kepastian hukum bagi pelaku bisnis jauh lebih penting, karena tidak hanya menyangkut transaksi tapi juga keamanan dalam berbisnis. Saat ini, bisnis berbasis elektronik sudah menjadi budaya internasional sehingga mau tidak mau pelaku bisnis harus mengikuti tren tersebut. Dengan belum adanya landasan hukum bidang TI (*cyber law*) di Indonesia sebetulnya merupakan satu titik lemah bagi industri TI, karena investor pasti enggan menanamkan investasinya jika tidak ada kepastian hukum.

Selain belum adanya UU yang mengatur tentang kejahatan siber, pemerintah juga kesulitan dalam pembuktian kasus *cyber crime*. Salah Sementara jumlah topik yang harus dibahas sangat banyak.

satu upaya yang dapat ditempuh adalah penelusuran bukti-bukti yang berkaitan dengan perbuatan pelaku cyber crime melalui jalur Kitab Undang-undang Hukum Acara Pidana (KUHAP). Artinya, disini tetap menggunakan alat-alat bukti berupa keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa.

III. PENUTUP

Perkembangan teknologi informasi khususnya di bidang telekomunikasi dan informasi, mempercepat proses globalisasi di semua aspek kehidupan. Fenomena ini menyebabkan batas antar negara semakin kabur, karena hubungan melalui dunia maya (*cyber space*) dapat dilakukan setiap saat.

Masyarakat dunia dalam menyikapi perkembangan teknologi dipenuhi oleh nuansa kebebasan, sehingga berbagai cara dilakukan untuk memperoleh kebebasan, bahkan terkadang dilakukan dalam bentuk yang bertentangan dengan dengan hukum, norma dan etika bermasyarakat.

Pengaruh tersebut menciptakan sebuah dimensi negatif yaitu kejahatan di bidang teknologi (*cyber crime*). Kejahatan di dunia maya adalah kejahatan yang amat sulit dibendung, karena penunjangnya adalah teknologi dan komunikasi. Sedangkan teknologi dan komunikasi menjadi unsur pendukung utama perkembangan dunia maya.

Kalau seandainya kejahatan di dunia maya terus dibiarkan, dampaknya tidak hanya akan mengganggu dunia maya tetapi juga dapat mengganggu kehidupan nyata.

Kasus-kasus yang muncul dalam cyber crime tidak dapat ditampung lagi oleh hukum, melalui UU dan peraturan yang sudah ada, sehingga dibutuhkan formulasi hukum baru yang menyangkut dunia maya ini. Instistusi penegak hukum perlu mempelopori dan merekomendasi lahirnya sebuah produk hukum yang mengatur tentang Dunia maya atau cyber law, sebagai bagian dari ikut sertanya dalam pembangunan hukum dan politik kriminal Indonesia.

Karena hadirnya unsur kecanggihan keahlian, maka perlu dibentuk suatu cyber police yang khusus menangani cyber crime, agar lebih mampu dan trampil, serta profesional menurut standar internasional bersama-sama dengan kepolisian manca negara sehingga mampu mengatasi persoalan-persoalan hukum cyber baik yang bersifat nasional, regional maupun internasional.

Untuk mempercepat pembentukkan *cyber police*, rekrutmen terhadap personel diambil dari masyarakat yang memiliki kemampuan khusus di bidang komputer dan seluk beluk operasional internet.

Dengan adanya perangkat hukum di dunia maya (*cyber law*) di Indonesia, teknologi informasi dapat terus berkembang pesat tanpa diikuti pengaruh negatif yang mendorong munculnya kejahatan komputer di dunia maya (*cyber crime*).

DAFTAR PUSTAKA

Chandraleka, Happy. 2004. Virus, Worm dan Trojan Horse. PT. Andi Offset. Yogyakarta.

Jovan, FN. 2006. Pembobol Kartu Kredit, Menyingkap Teknik dan Cara Kerja Carder di Internet. PT. Mediakita. Jakarta.

Ramli, M, Ahmad, Prof, Dr, SH,MH. 2004. Cyber Law dan HAKI Dalam Sistem Hukum Indonesia. PT. Refika Aditama. Bandung.

Ruslim, Harianto, CEH. 2006. Hack, Konsep, Penerapan dan Pencegahan. PT. Jasakom. Jakarta.

Sto. 2007. Seni Teknik Hacking Uncensored 2. PT. Jasakom. Jakarta.

Sutarman, Drs, MH. 2007. Cyber Crime, Modus Operandi dan Penanggulangannya. PT. LaksBangPRESSindo. Yogyakarta.

Susanto, Drs, Irjen Pol. 2005. Cyber Crime, Motif dan Penindakan. PT. Grafika Indah. Jakarta.