Faktor Exacta 6(1): 43-50, 2013
ISSN: 1979-276X

KESIAPAN APARATUR PEMERINTAH DALAM MENGHADAPI CYBER CRIME DI INDONESIA

RUDI HERMAWAN
rh001unindra@gmail.com
Program Studi Teknik Informatika, Fakultas Teknik, Matematika dan IPA
Universitas Indraprasta PGRI Jakarta

Abstrak. Cyber crime merupakan bentuk kejahatan yang terjadi pada dunia maya atau internet. Munculnya beberapa kasus kejahatan internet "CyberCrime" di Indonesia seperti, penyusupan-penyerbuan-perubahan terhadap situs target dapat menyebabkan kondisi abnormal terhadap situs korbannya (1), pembobolan kartu kredit dan penipuan perdagangan online (e-commerce) (2), dan pencemaran nama baik yang dilakukan melalui media online atau jejaring sosial (3). Maraknya kasus cyber crime ini telah menjadi kejahatan yang serius, sehingga pemerintah khususnya aparat hukum harus bisa mengimbangi kemampuan teknisnya untuk dapat mngungkap dan menangani para pelaku bila terjadi kasus cyber crime dan yang terpenting juga kemampuan untuk dapat mengadili pelaku cyber crime dengan menyiapkan payung hukum yang tepat dan tegas agar mampu menjerat dan menghukum para pelaku cyber crime. UU ITE saat ini yang digunakan sebagai payung hukum masih perlu di kaji dan di revisi melihat perkembangan dunia IT yang sangat pesat pertumbuhannya.

Kata kunci: cyber crime, internet, keamanan komputer, kesiapan pemerintah, UU ITE.

Abstract. Cyber crime is a form of crime that occurs in cyberspace or the internet. The emergence of several cases of internet crime "cybercrime" in Indonesia such as, intrusion-raid-change to a target site resulting in an abnormal condition of the victim site (1), credit card fraud and deception online commerce (e-commerce) (2), and libel whether conducted through online media or social networking (3). Rampant cases of cyber crime has become a serious crime, so that the government, especially law enforcement agencies should be able to offset the technical ability to be able to uncover and deal with the perpetrators in cases of cyber crime and most importantly the ability to be able to prosecute the perpetrators of cyber crime by setting up appropriate legal protection and decisively in order to be able to trap and punish the perpetrators of cyber crime. UU ITE is currently being used as an umbrella law is still necessary in the review and revision of the IT world saw very rapid.

Keywords: cyber crime, internet, computer security, government readiness, UU ITE.

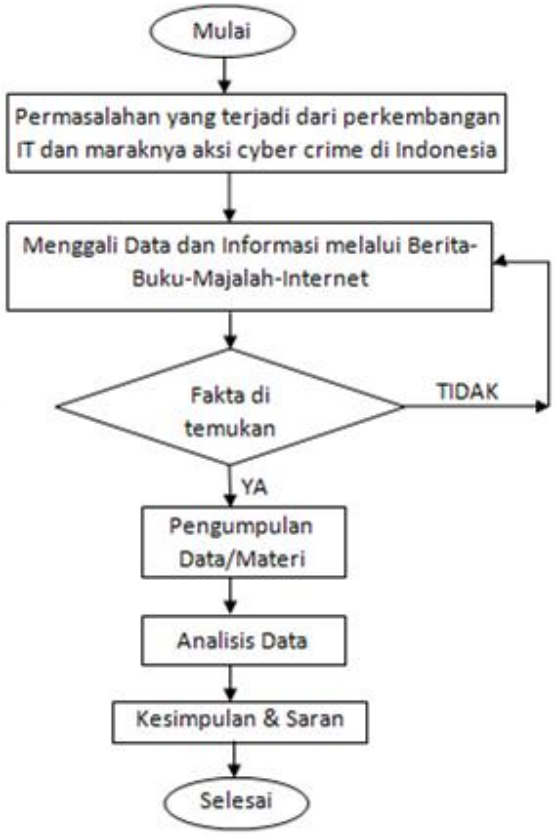
PENDAHULUAN

Sekarang ini, Teknologi Informasi Dan Komunikasi mengalami pertumbuhan yang sangat pesat, baik di Indonesia mau pun di seluruh dunia. Kemajuan teknologi informasi khususnya media internet, dirasakan banyak sekali memberikan manfaat positif bagi penggunanya seperti: Kecepatan dalam mengirim dan menerima informasi, kemudahan dalam melakukan aktifitas online, Mempermudah dalam transaksi bisnis, Sosial network yang sangat menyenangkan, Hiburan permainan tanpa batas. Pemanfaatan dan penggunaan teknologi internet juga tidak dapat dipungkiri juga membawa dampak negatif yang tidak kalah banyak dengan manfaat positif. Munculnya kasus kejahatan di dunia maya (cyber crime) seperti; Maraknya kasus pembobolan kartu kredit melalui aktifitas transaksi bisnis e-commerce, Banyaknya kasus penyusupan dan penyerangan ke

beberapa situs saat iniyang sering menjadi korban adalah situs pemerintah, dibidang akademik maraknya kasus plagiasi dalam dunia penciptaan karya ilmiah, dan juga banyaknya kasus Pencemaran nama baik akibat semakin bebas dan mudahnya semua orang dalam mengakses dan mempublikasikan berita maupun keluhan di forum-forum maupun di sosial media.

Manfaat dari penulisan ini adalah agar kita sebagai pengguna internet dapat memahami dan mengetahui sepak terjang para pelaku cyber crime secara lebih detail. Kita juga bisa mengetahui kesiapan dan strategi apa yang dilakukan pemerintah terhadap penanganan aksi kejahatan cyber crime di Indonesia. Serta kita bisa memahami sanksi dan ancaman hukuman bagi pelaku cyber crime dengan perundang-undangan yang berlaku di Indonesia.

Adapun tujuan penulisan ini diharapkan kita semakin mengetahui segala hal tentang dunia Cybercrime, mengetahui berbagai kasus Cybercrime yang terjadi di Indonesia, mengetahui bagaimana Penanganan pemerintah, mengetahui peranan kepolisian dalam menangani kasus cyber crime, mengetahui apakah efektif penerapan hukum dan Undang-Undang ITE terhadap kasus-kasus cyber crime di Indonesia.



Gambar 1. Kerangka Pemikiran

PEMBAHASAN

B. Simandjuntak mengatakan, *KEJAHATAN* merupakan suatu tindakan anti sosial yang dapat merugikan, tidak pantas, dan tidak dapat dibiarkan karena dapat menimbulkan kegoncangan dalam masyarakat. Indra Safitri mengemukakan, *CYBER CRIME* adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi dapat mengendalikan tingkat keamanan tinggi dan kredibilitas dari sebuah informasi yang

disampaikan dan di akses oleh pelanggan internet. Menurut Kepolisian Inggris, *CYBER CRIME* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.

Cybercrime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Beberapa pendapat mengindentikkan *cybercrime* dengan *computer crime. cybercrime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan akses internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

Berdasarkan jenis aktifitas yang dilakukannya, cybercrime dapat digolongkan menjadi beberapa jenis:

Hacking adalah kegiatan menerobos program komputer milik orang/pihak lain. Hacker adalah orang yang gemar eksplorasi/ngoprek komputer, memiliki keahlian membuat dan membaca program tertentu, dan terobsesi mengamati keamanan (security)-nya. "Hacker" memiliki 2 wajah ganda: "HACKER BUDIMAN/WHITE HAT HACKER" memberi tahu kepada admin yang komputernya diterobos, bahwa adanya kelemahan-kelemahan pada program yang dimiliki dan punya potensi disusup. Karakteristik White Hat Hacker ini adalah memberikan informasi bukan merusak yang pasti menguntungkan/membantu korbannya. "HACKER PENCOLENG/BLACK HAT HACKER", menerobos program orang lain untuk merusak, manipulasi/merubah serta mencuri datanya. Karakteristik Black Hat Hacker ini adalah melakukan aktifitas kriminal yang pasti merugikan korbannya.

Cracking adalah hacking untuk tujuan jahat. Sebutan pelaku cracking adalah "cracker" Aktfitas Cracker sejenis dengan "hacker bertopi hitam" (BLACK HAT HACKER). Berbeda dengan "carder" yang hanya mengintip kartu kredit, "cracker" mengintip simpanan para nasabah di berbagai bank atau pusat data sensitif lainnya untuk keuntungan diri sendiri. Meski sama-sama menerobos keamanan komputer orang lain, "hacker" lebih fokus pada prosesnya. Sedangkan "cracker" lebih fokus untuk menikmati hasilnya. Contoh kasus ini misalnya FBI bekerja sama dengan polisi Belanda dan polisi Australia menangkap seorang cracker remaja yang telah menerobos 50 ribu komputer dan mengintip 1,3 juta rekening berbagai bank di dunia. Dengan aksinya, "cracker" bernama Owen Thor Walker itu telah meraup uang sebanyak Rp 1,8 triliun. "Cracker" 18 tahun yang masih duduk di bangku SMA itu tertangkap setelah aktivitas kriminalnya di dunia maya diselidiki sejak 2006

Carding adalah Aktifitas berbelanja secara online tertapi menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal, pelaku carding biasa disebut carder. Biasanya para carder mencuri data nasabah dengan menginjeksi komunikasi data pada outlet atau store yang sering melakukan transaksi trading menggunakan kartu kredit. Menurut riset Clear Commerce Inc, perusahaan teknologi informasi yang berbasis di Texas – Amerika Serikat, Indonesia memiliki "carder" terbanyak kedua di dunia setelah Ukraina. Sebanyak 20 persen transaksi melalui internet yang berasal dari Indonesia adalah hasil carding. Akibatnya, banyak situs belanja online yang memblokir IP address (alamat komputer internet) yang berasal dari Indonesia. Menurut ICT Watch, Lembaga Swadaya Masyarakat yang mengamati dunia internet di Indonesia, para carder sekarang beroperasi semakin jauh, carder juga melakukan penipuan melalui forum-forum di milis dan ruang chatting di mIRC. Caranya para carder menawarkan barang-barang hasil carding nya dengan harga murah di channel. Misalnya, laptop dijual sangat murah dibawah harga pasar. Setelah ada yang orang berminat, carder akan meminta pembeli mengirim uang ke rekeningnya. Setelah Uang berhasil di transfer, barang tak pernah dikirimkan.

Defacing adalah merupakan kegiatan mengubah halaman situs/website pihak lain, seperti yang terjadi pada situs Presiden SBY, Kemenkominfo dan Partai Golkar, BI dan situs KPU saat pemilu 2004 lalu. Banyaknya kasus deface saat ini yang bermotif iseng belaka mereka ingin unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga pelaku deface yang jahat, mereka melakukan aktifitas deface untuk mencuri data dan dijual kepada pihak lain. Yang terjadi Hampir semua Kasus DEFACE di Indonesia berlatar belakang iseng dan unjuk kebolehan.

Fishing atau Phising adalah kegiatan memancing pengguna internet dengan harapan agar user secara tidak sadar memberikan informasi data user dan password nya pada website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online internet banking. Targetnya adalah nasabah yang ingin bertransaksi internet banking yang kurang teliti dalam menulis alamat website. Cara kerjanya Peretas biasanya membeli banyak domain plesetan dari bank yang menjadi target, sasarannya user merasa tidak menyadari telah salah mengetik alamat website namun tetap halaman awal website target dibuat sama seperti aslinya, akibat yang diharapkan oleh peretas nasabah mengisi User Id dan password. Setelah mengakses nasabah akan diberikan informasi gangguan terhadap server bank target, padahal itu bagian dari rekayasa peretas untuk membuat nasabah tidak menyadari kalau user dan passwordnya sudah diretas diambil oleh penyusup.

Spamming adalah pengiriman berita atau iklan lewat surat elektronik (e-mail) yang tak dikehendaki. Spam sering disebut juga sebagai bulk email atau junk email alias "sampah". Meski demikian, banyak juga orang yang terkena dan menjadi korbannya. Modus spamming yang paling sering adalah pengiriman e-mail mendapat hadiah, lotere, atau orang yang mengaku punya rekening di bank di Afrika atau Timur Tengah, minta bantuan "netters" untuk mencairkan, dengan janji bagi hasil. Apabila ada korban yag tertarik kemudian korban diminta nomor rekeningnya, dan mengirim uang/dana sebagai dana pemancing. Seorang rektor universitas swasta di Indonesia pernah diberitakan tertipu hingga Rp1 miliar karena kasus spamming seperti ini.

Kasus Cybercrime Di Indonesia Dan Penanganan Pemerintah

Kasus Defacing, Situs milik KPU (Komisi Pemilihan Umum) Defacing oleh hacker. Peristiwa tersebut terjadi pada tanggal 17 April 2004 dengan target situs *http://tnp.kpu.go.id*. Tampilan lambang 24 partai diganti dengan nama partai lucu 'partai jambu', 'partai cucak rowo', 'Partai Kolor Ijo' dan lainnya. Pelakunya, diketahui, bernama Dani Firmansyah 24 tahun mahasiswa asal Yogyakarta yang kemudian ditangkap Polda Metro Jaya. Motivasi pelaku, hanya ingin menjajal sistem pengamanan di server KPU yang dibeli sangat mahal dan anti bobol katanya saat itu. Tapi ternyata berhasil di tembus oleh Dani. Ketiadaan undang-undang cyber di Indonesia membuat Dani Firmansyah dijerat dengan pasal-pasal UU No 36/1999 tentang Telekomunikasi mengancam pidana terhadap perbuatan: memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan eletromagnetik terhadap penyelenggaraan telekomunikasi ". Dani Firmansyah, juga dijerat melakukan tindak pidana yang melanggar pasal 22 huruf a, b, c, Pasal 38 dan Pasal 50 UU No 36 tahun 1999 tentang Telekomunikasi. Pada pasal 22 UU Telekomunikasi berbunyi: Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi akses ke jaringan telekomunikasi dan atau akses ke jasa telekomunikasi; dan atau akses ke jaringan telekomunikasi khusus. Sedangkan bunyi pasal 50 UU No 36/1999 tentang Telekomunikasi 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 Rp 600.000.000,00 (enam ratus juta rupiah)."

Kasus Phising, Kasus klikbca merupakan kasus domain name yang memanfaatkan kesalahan ketik yang bisa dilakukan oleh para nasabahnya. Steven Haryanto membeli 5 domain plesetan pada situs target *www.klikbca.com yakni wwwklikbca.com, kilkbca.com, clikbca.com, klickbca.com* dan *klikbac.com*. Target dari Steven Haryanto adalah nasabah BCA yang melakukan salah ketik dalam penulisan klikbca, tampilan homepage web plesetan sama persis dengan homepage BCA. User akan melakukan login disitus-situs phising tsb, user name dan PIN internet korban akan terkirim pada sang pemilik situs. Steven Haryanto yang sudah meminta maaf dan menyerahkan semua user ID dan PIN kepada BCA. Kasus tsb tidak dilanjutkan ke pengadilan karena Steven memberikan informasi security BCA yang masih lemah. Saat itu pihak BCA tengah memikirkan alternatif lain ketimbang melaporkan Steven ke polisi. Steven Haryanto merupakan contoh karakteristik *WHITE HAT HACKER*.

Kasus Pornografi, Awal Juni 2010 publik dikejutkan dengan munculnya tiga buah video mesum tiga artis ibu kota, yaitu Nazriel Irham (Ariel), Luna Maya dan Cut tari. Dalam pengakuannya Ariel mengatakan bahwa ia merasa kecolongan atas file pribadi yang diperuntukkan untuk dikonsumsi secara pribadi. Namun, hukum pun harus berjalan. Ariel dijerat pasal 27 ayat (3) UU ITE No.11 Tahun 2008 berbunyi *Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.* Ariel juga di jerat Pasal 29 UU Pronografi: *Setiap orang yang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi sebagaimana dimaksu.* Majelis Hakim Pengadilan Negeri Bandung menjatuhkan hukuman 3,5 tahun penjara kepada Ariel dalam kasus video asusila tsb.

Kasus Pencemaran Nama Baik, Prita Mulyasari merupakan seorang ibu rumah tangga, Dia adalah mantan pasien Rumah Sakit Omni Internasional Alam Sutra Tangerang. Kasus ini terjadi saat ia dirawat di Rumah Sakit tersebut Prita tidak mendapat kesembuhan namun penyakitnya malah bertambah parah. Pihak rumah sakit tidak memberikan keterangan yang pasti mengenai penyakit Prita, dan pihak Rumah Sakit tidak memberikan rekam medis yang diperlukan oleh Prita. Kemudian Prita Mulyasari mengeluhkan pelayanan rumah sakit tersebut melalui email yang kemudian menyebar ke berbagai mailing list di dunia maya. Pihak Rumah Sakit Omni Internasional marah, dan merasa dicemarkan nama baik nya oleh Pita. Pihak RS Omni International mengadukan Prita Mulyasari secara pidana. Prita terjerat Undang-undang Nomor 11 Tahun 2008, Pasal 27 ayat 3 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam pasal tersebut tertuliskan: "*Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/ atau mentransmisikan dan/ atau membuat dapat diaksesnya Informasi Elektronik dan /atau Dokumen Elektronik yang memiliki muatan penghinaan dan/ atau pencemaran nama baik".* Pasal 27 ayat 3 ini kemudian menurut para Ahli hukum dan praktisi ICT sering disebut pasal karet, Kedua kata kunci di pasal itu adalah "*dengan SENGAJA*" dan "*TANPA HAK*". Menurut banyak pakar, Prita *Tidak Dengan Sengaja* mau menghina atau mencemarkan nama baik karena ia hanya menyampaikan keluhan mengenai apa yang ia alami, Hak tsb juga diatur dalam UU Perlindungan Konsumen." Pertanyaan berikutnya, apakah Prita memang *tak punya hak*? Prita *PUNYA HAK* untuk menyampaikan keluhan mengenai apa yang dialaminya. Karena Prita merupakan konsumen ia adalah pasien dari rumah sakit tsb. Adanya Kasus ini akan membawa dampak sangat buruk dan membuat masyarakat takut menyampaikan pendapat, kritik, saran atau komentarnya di dunia maya. Pasal UU ITE ini harus direvisi, setidaknya tidak boleh dipakai sebagai rujukan hukum

hingga nanti terbit PP (Peraturan Pemerintah) dan Permen/Kepmen Kominfo yang menjadi turunan hukumnya.

Peretasan Situs Negara *www.presidensby.info*, Pada 9 Januari 2013 situs *www.presidensby.info* di retas. Saat diretas, Halaman depan diganti dengan latar belakang hitam dengan tulisan warna hijau di bagian atas "Hacked by MJL007", sementara di bawahnya tertera sebuah logo dan tulisan "Jemberhacker Team" berwarna putih. Wildan ditangkap setelah menDEFACE situs SBY *www.presidensby.info* Wildan Yani S (22 th) peretas situs SBY lulusan SMK tahun 2010, Wildan memang tidak melanjutkan kuliah karena terhambat biaya. Wildan bekerja sebagai operator warung Internet di Jember. Wildan ditangkap pada 25 Januari lalu, terancam dengan melanggar Pasal 50 *juncto* Pasal 22 huruf b Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Wildan terancam hukuman pidana penjara paling lama 6 tahun penjara dan atau denda paling banyak Rp 600 juta. Wildan juga dinilai melanggar Pasal 46 Ayat (1), (2), dan (3) *jo* Pasal 30 Ayat (1), (2), dan (3) serta Pasal 48 Ayat (1) *juncto* Pasal 32 Ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Serangkaian pasal itu mengancam Wildan dengan hukuman penjara 6 hingga 10 tahun serta denda mencapai Rp 5 miliar. Namun, Kepolisian menganggap motif Wildan hanya iseng mengganti tampilan situs tersebut tanpa ada maksud politik. Bareskrim POLRI mengatakan, Wildan akan direkrut sebagai staf *cyber crime* MABES POLRI. Tetapi Kepolisian tetap memproses kasus Wildan. Saat ini sedang tahap penyelesaian perkara. Penangkapan Wildan ini kemudian memicu reaksi dari kelompok *hacker* internasional terkemuka, *ANONYMOUS*. Mereka meminta wildan di bebaskan dari segala tuntutan karena aksi wildan tidak merusak sistem maupun datanya tapi bersifat memberitahu dan mengingatkan bahwa pengelolaan situs penting milik pemerintah belum maksimal menjaga keamanannya, bila tuntutannya tidak dipenuhi mereka menyatakan "perang" terhadap situs Pemerintah Republik Indonesia dengan menumbangkan situs-situs berdomain "go.id". Situs-situs yang sudah dilumpuhkan antara lain beberapa sub domain di situs KPPU, BPS, KBRI Tashkent, Kemenkumham, Depsos, dan Kemenparekraf, bahkan Indonesia.go.id

Kemampuan pemerintah dan aparat kepolisian melawan cyber crime.

Kemampuan penyidik, Secara umum penguasaan dan pemahaman terhadap hacking komputer dari para penyidik Polri masih sangat minim. Banyak faktor yang mempengaruhi hal tersebut adalah Kurangnya pengetahuan ilmu IT dan belum memahami teknik hacking, modus-modus operandi para hacker dan profil-profilnya serta metode penyerangannya. Sebagian besar dari penyidik minim Pengetahuan dan pengalaman dalam menangani kasus-kasus cyber crime pun masih terbatas jam terbangnya. Faktor sistem pembuktian yang menyulitkan para penyidik karena Jaksa (Penuntut Umum) masih meminta keterangan saksi dalam bentuk Berita Acara Pemeriksaan (BAP) formal harus hadir secara fisik, sehingga diperlukan pemanggilan saksi/korban yang berada di luar negeri untuk dibuatkan berita acaranya di Indonesia, Hukum di Indonesia belum bisa menerima pernyataan korban atau saksi *dalam bentuk faksimili atau email* sebagai *alat bukti*. Selama ini dalam menangani kasus cyber crime Aparat hukum masih meminta bantuan para pakar IT untuk mengungkap pelaku cyber crime.

Strategi Penanganan Pemerintah

Penyempurnaan perangkat hukum, Polri, Kemenkominfo, DPR, pakar hukum dan organisasi lainnya yang sangat berkepentingan atau keamanan usahanya tergantung dari kesempurnaan undang-undang di bidang cyberspace (pengusaha *e-commerce* dan

banking) sedang memproses untuk merancangnya agar di Indonesia terwujud UU ITE yang sempurna. UU ITE diharapkan bersifat lex specialist, menyempurnakan undang-undang pendukungnya dan melakukan sintesa serta analogi yang lebih luas terhadap KUHP. UU ITE yang sudah ada perlu direvisi terutama pasal / ayat yang karet (multi tafsir), setidaknya tidak boleh dipakai sebagai rujukan hukum hingga nanti terbit PP dan Permen/Kepmen Kominfo yang menjadi turunan hukumnya. Perlu dilakukan Komitmen dan kerja sama yang intensif antara Kemenkominfo dengan para pakar dari universitas-universitas dan pelaku bisnis ICT *khususnya ISP dan* Computer Network Security dalam mengantisipasi perkembangan cyber crime di Indonesia.

Mendidik para penyidik, Dalam hal menangani kasus cybercrime diperlukan penyidik yang mempunyai cukup pengalaman (bukan penyidik pemula), pendidikannya diarahkan untuk menguasai teknis penyidikan dan menguasai administrasi penyidikan serta dasar-dasar pengetahuan di bidang komputer dan profil hacker. Untuk itu diperlukan pengiriman aparat hukum Polisi, Jaksa, Hakim untuk melakukan pendidikan mengenai cyber crime di negara maju khususnya Amerika Serikat.

Membangun Fasilitas Forensic Computing, Keberadaan Fasilitas Forensic Computing sangat penting dan vital dalam membongkar kasus cyber crime. Fasilitas Forensic Computing yang akan didirikan Polri diharapkan akan dapat melakukan tiga hal penting, yaitu; Evidence Collection (pengumpulan bukti), Forensic Analysis (analisis forensik), Expert Witness (saksi ahli). Diharapkan nantinya Para ahli forensik komputer bisa memanfaatkan fasilitas tsb untuk mendeteksi lokasi kejahatan yang tepat dan juga mendukung dalam pemulihan dokumen yang hilang atau sengaja dirusakkan. Ahli Komputer forensik menangani dengan setiap kasus dengan sangat hati-hati ketika akan melakukan pemeriksaan forensik, Setiap melakukan kesalahan penempatan akan berakibat korupsi data atau dapat merusak sistem secara keseluruhan. Komputer forensik memungkinkan ahli forensik dapat mengetahui masing-masing dari setiap file. Baik file yang disimpan di tempat biasa dan maupun yang tersembunyi dan file yang dilindungi oleh security. Hal tersebut dapat dilakukan melalui tool forensik. Forensik komputer ini juga memainkan peran sebagai analisa teknis sehingga mampu menyelidiki bagian yang paling sulit terjangkau dari perangkat digital.

Meningkatkan Upaya Penyidikan Dan Kerja Sama Internasional, Indonesia melalui Kepolisian RI bekerja sama dengan Amerika Serikat (AS) melalui International Criminal Investigative Training Assistance Program (ICITAP) melatih lebih dari 100 orang polisi se-Jawa timur mengenai cara mengatasi "Cyber Crime" (Tindak Kejahatan Dunia Maya). Selain itu Aparatur kepolisian melalui Kepolisian negara-negara Asean terus berkoordinasi dan bekerjasama untuk memerangi kejahatan di dunia maya atau cyber crime. Untuk meningkatkan kemampuannya, sebanyak 70 perwira dari kepolisian se Asean mengikuti pelatihan selama dua hari di Bandung. pelatihan ini juga melibatkan para ahli dari Interpol, Apcert, Microsoft, kepolisian Korea dan Kepolisian Federal Australia. Kerjasama Kepolisian Republik Indonesia (Polri) dengan Australia Federal Police (AFP), dalam bidang penanganan kejahatan cyber, diharapkan mampu meningkatkan kinerja penyidik dalam menangani bukan hanya kasus cyber crime, namun juga terorisme di Indonesia.

PENUTUP

Kesimpulan

Cybercrime merupakan permasalahan yang harus ditangani secara hati-hati dan serius karena dampak dari kejahatan ini sangat luas dan bisa merugikan perekonomian masyarakat, apabila tidak ditanggulangi akan berkembang serta tidak terkendali dan dampaknya bisa sangat fatal bagi kehidupan bermasyarakat. Kendala utama yang

dihadapi aparatur negara dalam penyelidikan *cybercrime* antara lain *borderless (tak terbatas)* baik korbannya maupun tersangkanya sehingga perangkat hukum konvensional yang ada di Indonesia belum atau tidak bisa menjangkau secara efektif. Diperlukan peralatan *FORENSIK COMPUTING* yang canggih guna pembuktian kejahatan cyber, serta menyiapkan penyidik Polri untuk dididik agar mampu menyidik *cybercrime* serta kerja sama dengan penegak hukum yang ada di luar negeri.

Saran

UU ITE sebagai landasan utama bagi penegak hukum untuk menjerat setiap pelaku tindak pidana khusus nya kejahatan internet (cybercrime), namun UU tersebut terkesan sangat mendesak dibuat tanpa melihat sebesar apa potensi dan kemampuan hukum untuk menghadapi masalah cybercrime. Perlu diwujudkan hukum turunannya Permen (peraturan Menteri) untuk mempertajam agar tidak menimbulkan celah yang multi tafsir. Aparat polisi cyber diharapkan anggotanya bukan hanya dari jajaran kepolisian saja sebaiknya membuka kesempatan bagi para hacker yang paham tentang kejahatan dunia maya di recrut juga, tentu hal ini sangat bermanfaat untuk mengungkap & menanggulangi cybercrime diIndonesia. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties. Perlunya Adanya Lembaga Khusus Anti Cyber Crime: Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime. Dalam menanggulangi kasus pornografi sebaiknya pemerintah bekerjasama secara intensif dengan para pakar IT, pakar pendidikan dan LSM ICT Watch serta Lembaga Perlindungan Anak (LPAI) untuk membuat daftar hitam terhadap situs yang mengandung konten pornografi, Daftar situs tsb terus di update dan disebarluaskan kepada setiap ISP, penyedia layanan jasa internet, perusahaan pengembang filter/*software* dan operator mobile phone.

DAFTAR PUSTAKA

Garda T. Paripurna. 2008. **Sekilas Tentang Kejahatan Transnasional, Riset Hukum Kejahatan Transnasional.**

Petrus Reinhard Golose, **Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia Oleh Polri**, Makalah pada Seminar Nasional tentang "Penanganan Masalah Cybercrime di Indonesia dan PengembanganKebijakan Nasional yang Menyeluruh Terpadu", diselenggarakan oleh Deplu,BI, dan DEPKOMINFO, Jakarta, 10Agustus 2006, hal 5

http://www.balitbang.kemhan.go.id/?q=content/cybercrime-sebagai-dampak-perkembangan-teknologi-informasi

http://diskominfo.jabarprov.go.id/70-perwira-polisi-negara-asean-dilatih-perangi-kejahatan-dunia-maya/#.UaIR50NrW1s

http://nasional.kompas.com/read/2013/01/30/22222727/Wildan.Retas.Situs.Presiden.SBY.Sendirian

http://ono32.wordpress.com/2010/07/25/apa-dan-bagaimana-carding-penanganan-tindak-pidana-cybercrime-di-indonesia/

http://www.tempo.co/read/news/2013/03/26/063469439/Wildan-Peretas-Situs-SBY-Dijerat-Undang-Undang-ITE