“PENEGAKAN HUKUM CYBERCRIME di INDONESIA”

1. **Penagakan Hukum**  Penagakan hukum adalah kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan didalam kaidaha-kaidah atau pandangan-pandangan nilai yang mantap dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir untuk menciptakan, memelihara dan mempertahankan kedamaian pergaulan hidup.

Penegakan hukum secara konkrit adalah berlakunya hukum positif dalam praktek sebagaimana seharusnya patut ditaati.

Secara umum, sebagaimana yang dikemukakan oleh Soerjono Soekanto, ada lima faktor yang mempengaruhi penegakan hukum, yaitu:

a.    faktor hukumnya sendiri

b.    faktor penegak hukum, yaitu pihak-pihak yang memebentuk maupun yang menerapkan hukaum

c.    faktor sarana dsan fasilitas yang mendukung penegakan hukum

d.   faktor masyarakat, yaitu lingkungan dimana hukum itu berlaku dan diterapkan

e.    faktor kebudayaan, yakni sebagai hasil karya, cipta dan rasa yang didasarkan pada karsa manusia didalam pergaulan hidup.

**B. Pengertian Cybercrime** Cybercrime dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.   
  
 Tiga pendekatan untuk mempertahankan keamana di syberspace. Pertama adalah pendekatan teknologi. Kedua, pendekatan sosial, budaya dan etika. Ketiga, pendekatan hukum. Untuk mengatasi ganguan keamanan, prndekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan mudah disusupi, diintersepsi, atau diakses secara ilegal dan tanpa hak  
   
**C. Jenis Cybercrime**  
 Cybercrime dapat dilihat dari dua sudut pandang:

1. Kejahatan yang menggunakan teknologi informasi sebagai fasilitas.

**Contoh** :pembajakan, pornografi, dan pemalsuan/pencurian kartu kredit

1. Kejahatan yang menjadikan sistem teknologi informasi sebagai sasaran.

**Contoh**:pencurian abstracts pribadi, pembuatan/penyebaran virus komputer, dan pembobolan/pembajakan situs

**D. Modus Operandi Cyber Crime** Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain:

1. Unauthorized Access

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

2. Illegal Contents

Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, seperti: penyebaran pornografi.

3. Penyebaran virus secara sengaja

Penyebaran virus pada umumnya dilakukan dengan menggunakan email.

4. Data Forgery

Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

5. Cyber Espionage, Sabotage and Extortion

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.

6. Cyberstalking

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang denganmemanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan ini menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentutanpa harus menyertakan identitas diri yang sebenarnya.

7. Carding

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

8. Hacking dan Cracker

. Cracker adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain,pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran.

9. Cybersquatting and Typosquatting

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal.

Typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain, yang merupakan nama domain saingan perusahaan.

10. Hijacking

Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain yang paling sering terjadi adalahSoftware Piracy (pembajakan perangkat lunak).

11. Cyber Terorism

Suatu tindakan cybercrime termasuk cyber terorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer.

**E. Karakteristik *cyber crime***

Berdasarkan beberapa literatur serta praktiknya, *cyber crime* memiliki beberapa karakteristik, yaitu :

1. Perbuatan yang dilakukan secara illegal, tanpa hak atau tidak etis tersebut terjadi dalam ruang atau wilayah siber atau *cyber (cyberspace)*, sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhdapnya.
2. Perbuatan tersebut dilakukan degan menggunakan peralatan apa pun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian materiil maupun immaterial (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan secara transnasional atau melintasi batas negara.

**F. Permasalahan Dalam Penyidikan Terhadap Cybercrime**

Adapun hambatan-hambatan yang ditemukan di dalam proses penyidikan antara lain adalah sebagai berikut:

1. Perangkat Hukum yang Belum Memadai

2. Kemampuan Penyidik

a.  Kurangnya pengetahuan tentang komputer.

b. Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus   
 cybercrime masih terbatas.

c. Faktor sistem pembuktian yang menyulitkan para penyidik..

**G. Upaya-Upaya Yang Dilakukan Oleh Pihak Kepolisian**

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

a. Personil

Polri mengirimkan anggotanya untuk mengikuti berbagai macam kursus di negara–negara maju   
 agar dapat diterapkan dan diaplikasikan di Indonesia,   
b.Sarana Prasarana  
 Perkembangan teknologi yang cepat juga tidak dapat dihindari, sehingga Polri berusaha   
 semaksimal mungkin untuk meng up date dan up grade sarana dan prasarana yang dimiliki, antara   
 lain Encase Versi 4, 2.  
c. Kerjasama dan Koordinasi  
 Melakukan kerjasama dalam melakukan penyidikan kasus kejahatan cyber karena sifatnya yang   
 borderless dan tidak mengenal batas wilayah, sehingga kerjasama dan koordinasi dengan aparat   
 penegak hukum negara lain merupakan hal yang sangat penting untuk dilakukan.  
d. Sosialisasi dan Pelatihan  
 Memberikan sosialisasi mengenai kejahatan cyber dan cara penanganannya kepada satuan di   
 kewilayahan (Polda) serta pelatihan dan ceramah kepada aparat penegak hukum lain (jaksa dan   
 hakim) mengenai cybercrime agar memiliki kesamaan persepsi dan pengertian yang sama dalam   
 melakukan penanganan terhadap kejahatan cyber terutama dalam pembuktian dan alat bukti yang   
 digunakan.  
 **H. Penegakan Hukum CyberCrime Di Indonesia**

**1. Kitab Undang Undang Hukum Pidana**

. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal - pasal yang dapat dikenakan dalam KUHP pada cybercrime antara lain:

1.**Pasal 362 KUHP** yang dikenakan untuk kasus carding

2 **Pasal 378 KUHP** dapat dikenakan untuk penipuan

3.**Pasal 335 KUHP** dapat dikenakan untuk kasus pengancaman dan pemerasan

4**.Pasal 311 KUHP** dapat dikenakan untuk kasus pencemaran nama baik

5.**Pasal 303 KUHP** dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia.

6.**Pasal 282 KUHP** dapat dikenakan untuk penyebaran pornografi

7. **Pasal 282 dan 311 KUHP** dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet

8**.Pasal 378 dan 262 KUHP** dapat dikenakan pada kasus carding, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.

9. **Pasal 406 KUHP** dapat dikenakan pada kasus deface atau hacking serta data interference

10. **Pasal 112, 113, 114, 115 dan 116 KUHP** dapat dikenakan pada perbuatan membocorkan dan memata-matai data atau informasi yang berisi tentang rahasia negara.

**2. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta**

Menurut Pasal 1 Undang - Undang No 19 Tahun 2002 tentang Hak Cipta, Hak cipta untuk program komputer berlaku selama 50 tahun, sebagai mana yang terdapat dalam Pasal 30. Harga program komputer atau software yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual software bajakan dengan harga yang sangat murah.

**3. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi**

Menurut Pasal 1 Undang-Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Penyalah gunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang- Undang ini:

1. Illegal access, perbuatan melakukan akses secara tidak sah terhadap sistem komputer ini belum diatur secara jelas di dalam sistem perundang-undangan di Indonesia. Untuk sementara waktu, Pasal 22 Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi dapat diterapkan.

**Pasal 22** Undang-Undang Telekomunikasi menyatakan:

“Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

a. akses ke jaringan telekomunikasi; dan/atau

b. akses ke jasa telekomunikasi; dan/atau

c. akses ke jaringan telekomunikasi khusus.”

**Pasal 50** Undang-Undang Telekomunikasi memberikan ancaman pidana terhadap barang siapa yang melanggar ketentuan Pasal 22 Undang-UndangTelekomunikasi dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah).

2. Illegal interception in the computers, systems and computer networks operation (intersepsi secara tidak sah terhadap operasional komputer, sistem, danjaringan komputer)**.**Pasal 40 Undang-Undang Telekomunikasi dapat diterapkan terhadap jenis perbuatan intersepsi ini.   Pasal 56 Undang-Undang Telekomunikasi memberikan ancaman pidana terhadap barang siapa yang melanggar ketentuan Pasal 40 tersebut dengan pidana penjara paling lama 15 (lima belas) tahun.  
**4. Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan**

Dengan dikeluarkannya Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan yang didalam ketentuan salah satu pasalnya mengatur mengenai di mungkinkannya penyimpanan dokumen perusahaan dalam bentuk elektronis (paperless) memberikan pengakuan bahwa dokumen perusahaan yang disimpan dimedia elektronik dapat dijadikan alat bukti yang sah.[[21]](http://www.blogger.com/post-create.g?blogID=2970737601005741979" \l "_ftn21" \o ")Misalnya: Compact Disk Read Only Memory (CD ROM), dan Write Once Read Many (WORM), yang diatur dalam Pasal 12 Undang-Undang tersebut sebagai alat bukti yang sah.

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

Undang-Undang ini merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian uang sebagai mana yang terdapat dalam pasal 2 ayat 1. Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang diatur dalam Undang-Undang Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau digital evidence sesuai dengan Pasal 38 yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu.

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

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

**7. Undang-Undang Nomor 11 Tahun 2008 Tentang Internet dan Transaksi Elektronik**

Undang-undang ini, yang telah disahkan dan diundangkan pada tanggal 21 April 2008, walaupun sampai dengan hari ini belum ada sebuah PP yang mengatur mengenai teknis pelaksanaannya, namun diharapkan dapat menjadi sebuah undang-undang cyber atau cyberlaw guna menjerat pelaku-pelaku cybercrime yang tidak bertanggungjawab dan menjadi sebuah payung hukum bagi masyarakat pengguna teknologi informasi guna mencapai sebuah kepastian hukum

1. **Upaya-Upaya Penyalahgunaan Penggunaan Komputer**

upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:[[1]](#footnote-1)

* 1. Melakukan Modernisasi hukum pidana material dan hukum acara pidana
  2. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer
  3. Melakukan langkah-langkah untuk membuat peka warga warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer
  4. Melakukan upaya-upaya pelatihan bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan ekonomi dan *cyber crime*
  5. Memperluas *rule of ethics* dalam penggunaan computer dan mengajarkannya melalui kurikulum informatika
  6. Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime.*

Menurut Agus Raharjo bahwa salah satu langkah lagi agar penanggulangan *cyber crime* ini dapat dilakukan dengan baik, maka perlu dilakukan kerja sama dengan *Internet Service Provider* (ISP) atau penyedia jasa internet. Meskipun *Internet Service Provider* (ISP) hanya berkaitan dengan layanan sambungan atau akses Internet, tetapi *Internet Service Provider* (ISP) memiliki catatan mengenai ke luar atau masuknya seorang pengakses, sehingga ia sebenarnya dapat mengidentifikasikan siapa yang melakukan kejahatan dengan melihat *log file* yang ada.[[2]](#footnote-2) Ada beberapa cara yang dapat digunakan untuk mengamankan sistem informasi berbasis internet yang telah dibangun yaitu sebagai berikut.26 a. Mengatur akses *(access control)*

Salah cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme *authentication* dan *access control.*

1. Menutup *service* yang tidak digunakan

Seringkali dalam sebuah sistem (perangkat keras dan atau perangkat lunak) diberikan beberapa servis yang dijalankan sebagai *default,* seperti pada sistem UNIX yang sering dipasang dari *vendor*-nya adalah *finger, telnet, ftp,* *smtp, pop, echo* dan sebagainya. Sebaiknya servis-servis ini kalau tidak dipakai dimatikan saja. Karena banyak kasus terjadi yang menunjukkan *abuse* dari servis tersebut atau ada lubang keamanan dalam servis tersebut. Akan tetapi *administrator* sistem tidak menyadari bahwa servis tersebut dijalankan di komputernya.

1. Memasang Proteksi

Proteksi ini bisa berupa *filter* (secara umum) dan yang lebih spesifik lagi adalah *firewall. Filter* ini dapat digunak untuk memfilter *e-mail,* informasi, akses atau bahkan dalam *level packet*. Sebagai contoh, di sistem UNIX ada paket program *topwrapper* yang dapat digunakan untuk membatasi akses kepada servis atau aplikasi tertentu. Misalnya, servis untuk *telnet* dapat dibatasi untuk sistem yang memiliki nomor IP tertentu atau memiliki *domain* tertentu. Sementara *firewall* digunakan untuk melakukan *filter* secara umum. Ada juga program *filter* internet yang bernama *ZeekSafe.* Program ini bisa memblokir situs-situs yang tidak diinginkan. Selain itu, ada juga program filter yang lain, yaitu *We-Blocker,* sama dengan *ZeekSafe,* program ini bisa menentukan parameter apa saja yang akan membatasi akses ke *website* yang dianggap tidak layak dilihat.

1. *Firewall*

Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang ke luar dan masuk harus melalui *firewall* ini. Tujuan utama dari *firewall* adalah untuk menjaga *(prevent)* agar akses (ke dalam maupun ke luar) dari orang tidak berwenang *(unauthorized access)* tidak dapat dilakukan. *Firewall* bekerja dengan mengamati paket *Internet Protocol* (IP) yang melewatinya. Berdasarkan konfigurasi dari *firewall,* maka akses dapat diatur berdasarkan *Internet Protocol* (IP) *address, port* dan arah informasi.

1. Pemantau adanya serangan

Sistem pemantau *(monitoring system)* digunakan untuk mengetahui adanya tamu tidak diundang *(intruder)* atau adanya serangan *(attack).* Nama lain dari sistem ini adalah *Intruder Detection System* (IDS). Sistem ini dapat memberi tahu administrator melalui *email* maupun melalui mekanisme lain seperti *pager.* Ada beberapa cara untuk memantau adanya *intruder,* baik yang sifatnya aktif maupun pasif.

1. Pemantau integritas sistem

Sistem ini dijalankan secara berkala untuk menguji integritas sistem. Salah satu contoh program yang umum digunakan di sistem UNIX adalah program *Tripwire.* Program ini dapat digunakan untuk memantau adanya perubahan pada berkas. Pada mulanya program ini dijalankan dan membuat data *base* mengenai berkas-berkas atau direktori yang ingin kita amati beserta *signature* dari berkas tersebut. *Signature* berisi informasi mengenai besarnya berkas, kapan dibuatnya, pemiliknya, hasil *checksum* atau *hash* dan sebagainya. Apabila ada perubahan pada berkas tersebut, maka keluaran dari *hash function* akan berbeda dengan yang ada di data *base* sehingga ketahuan adanya perubahan.

1. Audit: Mengamati berkas *log*

Segala kegiatan penggunaan sistem dapat dicatat dalam berkas yang biasanya disebut *log file* atu *log* saja. Berkas *log* ini sangat berguna untuk mengamati penyimpanan yang terjadi. Kegagalan untuk masuk ke sistem *(login)* misalnya tersimpan dalam berkas *log.* Untuk itu pada *administrator* diwajibkan untuk rajin memelihara dan menganalisis berkas *log* yang dimilikinya.

1. *Back up* secara rutin

Sering kali intruder masuk dalam sistem dan merusak sistem dengan menghapus berkas-berkas yang ditemui. Jika *intruder* ini berhasil menjebol sistem dan masuk sebagai *superuser,* maka ada kemungkinan dia dapat menghapus seluruh berkas. Untuk itu, adanya *back up* yang digunakan secara rutin merupakan hal yang esensial.

1. Penggunaan enkripsi untuk meningkatkan keamanan

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Banyak servis di internet yang masih menggunakan *plain text* untuk *authentication* seperti penggunaan pasangan *userid* dan *password.* Informasi ini dapat dilihat dengan mudah dengan program penyadap atau pengendus *(sniffer).* Untuk meningkatkan keamanan *server world wide web* dapat digunakan enkripsi pada tingkat *socket.* Dengan menggunakan *enkripsi,* orang tidak bisa menyadap data-data (transaksi) yang dikirimkan dari/ke *server* WWW.

Salah satu mekanisme yang cukup populer adalah dengan menggunakan *Secure Socket Layer* (SSL) yang mulanya dikembangkan oleh *Netscape.* Selain *server* WWW dari *Netscape* dapat juga dipakai *server* WWW dari *Apache* yang dapat dikonfigurasi agar memiliki fasilitas *Secure Socket layer* (SSL) dengan menambahkan *software* tambahan *SSLeay*-implementasi *Secure Socket Layer* (SSL) dari *Eric Young*-atau *Open Secure Socket Layer* (SSL). Penggunaan *Secure Socket Layer* (SSL) memiliki permasalahan yang bergantung kepada lokasi dan hukum yang berlaku. Hal ini disebabkan pemerintah melarang ekspor teknologi enkripsi

(kriptografi) dan paten *Public Key Partners* atas *Rivest-Shamir-Adleman*

(RSA) *public key* *cryptography* yang digunakan pada *Secure Socket Layer* (SSL). Oleh karena itu, implementasi *SSLeay Eric Young* tidak dapat digunakan di Amerika Utara (Amerika dan Kanada) karena melanggar paten *Rivest-Shamir-Adleman* (RSA) dan RC4 yang digunakan dalam implementasinya.

j. *Telnet* atau *shell* aman

*Telnet* atau *remote login* yang digunakan untuk mengakses sebuah *remote site* atau computer melalui sebuah jaringan computer. Akses ini dilakukan dengan menggunakan hubungan TCP/IP dengan menggunakan *user id* dan *password.* Informasi tentang *user id* dan *password* ini dikirimkan melalui jaringan komputer secara terbuka. Akibatnya kemungkinan *password* bisa kenak *sniffing.* Untuk menghindari hal ini bisa memakai enkripsi yang dapat melindungi adanya *sniffing.* Selain itu bisa juga memakai *firewall,* alat ini untuk melindungi data-data penting. Akan tetapi sistem pengamanan yang telah dipaparkan di atas tadi tidak menjamin aman 100% (seratus persen), oleh karena itu dianjurkan untuk terus memantau perkembangan sistem pengamanan internet.

Dari paparan penegakan hukum dengan sarana non-penal ini, maka membutuhkan penegak hukum yang menguasai teknologi informasi. Atau lebih jelasnya kita sangat membutuhkan Polisi *Cyber,* Jaksa *Cyber,* Hakim *Cyber* dalam rangka penegakan hukum *Cyber Crime* di Indonesia. Tanpa adanya penegak hukum yang mempuni di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat *cyber* oleh karena kejahatan *cyber* ini *locos delicti*-nya bisa lintas negara.

Sumber :   
<http://wahyuagungriyadiblog.blogspot.com/2011/03/kejahatan-cybercrime.html?m=1>  
Penegakan\_Hukum\_terhadap\_Cyber\_Crime\_di.Doc  
2331-5088-1-SM.PDF

1. Barda Nawawi Arief,*Op. Cit.,* hlm. 238-239. [↑](#footnote-ref-1)
2. Agus Raharjo,*Op. Cit.,*hlm. 248. 26 *Ibid,* hlm. 252-260. [↑](#footnote-ref-2)