PENEGAKAN HUKUM TERHADAP KEJAHATAN TEKNOLOGI INFORMASI (*CYBER CRIME*)

Pristika Handayani
Dosen Tetap Prodi Ilmu Hukum UNRIKA

ABSTRAK

Teknologi pada saat ini sudah semakin maju dan canggih. Seiiring dengan perkembangan jaman begitu pula teknologi juga mengalami kemajuan yang sangat pesat. Semakin canggihnya teknologi maka semakin canggih pula kejahatan yang bisa dilakukan manusia. Salah satunya adalah kejahatan di dunia teknologi informasi atau yang lebih dikenal dengan *cyber crime.* Kejahatan dunia maya ini sangat marak kita temui. Para pelaku kejahatan dengan mudah untuk melancarkan aksi dengan menggunakan teknologi informasi.

Cyber crime adalah merupakan kejahatan yang dilakukan dengan menggunakan teknologi informasi yaitu dengan menggunakan internet. Banyak cara yang bisa dilakukan para pelaku kejahatan dengan menggunakan internet. Kita harus lebih wapada lagi terhadap kerahasiaan data kita, karena bisa saja data kita tersebut akan disalahgunakan oleh oknum yang tidak bertanggungjawab.

Undang-undang yang mengatur mengenai *cyber crime* ini adalah KUHP (Kitab Undang-Undang Hukum Pidana) dan juga sekarang sudah ada undnag-undang yang secara khusus mengatur mengenai permasalahan kejahatan yang menggunakan teknologi informasi yaitu undang-undang informasi dan transaksi elektronik (ITE).

*Keywords: cyber crime,*Teknologi Informasi dan UU ITE

PENDAHULUAN

Fenomena *cyber crime di* Indonesia merupakan perbincangan yang selalu menarik minat masyarakat. Dari masyarakat pada umumnya, sampai pada masyarakat yang memang memiliki keterkaitan langsung dengan fenomena *cyber crime.* Misalnya, aparat penegak hukum, akademisi khususnya akademisi hukum. Dalam dunia akademisi hukum, perbincangan ini tambah menarik terkait dengan upanya pemerintah untuk menyusun peraturan perundang-undangan tentang *cyber crime*.

Kata teknologi yang berasal dari bahasa Yunani yaitu *technikos* yang berarti kesenian atau keterampilan dan *Logos* yaitu ilmu atau asas-asa utama. Kata teknologi mengandung arti bahwa ilmu dibelakang keterampilan atau asas-asas utama dari pada suatu keterampilan.[1]

Jika kita kaitkan kata teknologi dengan informasi yaitu mengandung makna bahwa teknologi informasi adalah suatu teknologi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan pemerintahan dan juga merupakan informasi yang strategis untuk pengambilan keputusan. Teknologi ini menggunakan seperangkat komputer untuk mengolah data, sistem jaringan untuk menghubungkan satu

[1] Abdul Wahid dan M. Labib, "*Kejahatan Mayantara (Cyber Crime)",* Refika Aditama, Bandung, 2005, Hal.15

komputer dengan komputer yang lainnya sesuai dengan kebutuhan dan teknologi telekomunikasi digunakan agar data dapat disebar dan diakses secara global.[2]

Di era globalisasi, perkembangan teknologi informasi dan komunikasi telah mengakibatkan semakin derasnya lalu lintas informasi. Akibatnya, akses terhadap informasi dan komunikasi semakin mudah didapatkan oleh setiap orang tanpa ada hambatan ruang dan waktu. Globalisasi dalam dunia ekonomi khususnya dunia perdagangan adalah salah satu aspek kehidupan yang mendapatkan imbas dari kehadiran media komunikasi yang cepat dan handal sehingga aktifitas bisnis diberbagai negara cenderung meningkat.[3]

Setelah menelaah lebih rinci mengenai pengertian teknologi informasi maka yang harus juga ketahui mengenai *cyber crime* juga. Kata *cyber crime* tidak begitu familiar ditelinga masyarakat. Kata *cyber crime* masih sangat jarang digunakan oleh masyarakat kita. Oleh karena itu agar kita tidak tertinggal dengan negara-negara lain dan memang seharusnya diketahui oleh masyarakat kita agar nantinya bisa mengantisipasi apabila terjadi sesuatu hal khususnya kejahatan dunia maya atau kejahatan mayantara dapat mencari solusi atau bantuan hukum dan juga jangan sampai melakukan kesalahan dikarenakan tidak mengetahui bahwa apa yang dilakukan adalah melanggar hukum.

Menurut kepolisisan Inggris *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.

Cyber crime itu sendiri adalah kejahatan yang dilakukan oleh seseorang maupun kelompok dengan menggunakan sarana komputer dan alat telekomunikasi lainnya. Seseorang yang menguasai dan mampu mengoperasikan komputer seperti operator, programmer, analis, manager, kasir juga dapat melakukan *cyber crime.* Cara yang bisa dilakukan dengancara merusak data, mencuri data, dan menggunakannya secara ilegal. Faktor yang dominan mendorong berkembangnya *cyber crime* itu sendiri adalah pesatnya perkembangan teknologi komunikasi seperti telepon, *handphone,* dan alat telekomunikasi lainnya yang dipadukan dengan perkembangan teknologi komputer.[4]

Jenis-jenis kejahatan *Cyber Crime*:

1. *Unauthorized Access to Computer System and Service*
   Kejahatan ini dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa ijin atau tanpa sepengetahuan dari pemilik jaringan komputer yang dimasukinya. Motifnya adalah bermacam-macam antara lain adalah sabotase, pencurian data dan sebagainya.

2. *Illegal Contens*
   Kejahatan ini dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu yang tidak benar, tidak etis dan dapt dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh yang termasuk kejahatan jenis ini adalah pornografi, pemuatan berita bohong, termasuk juga delik-delik politik dapat dimasukkan kedalam kategorgi ini bila menggunakan ruang *cyber.*

3. Data *Forgery*
   Yaitu merupakan kejahatan dengan cara memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai dokumen melalui internet.

---

[2] Sulistyo Basuki "*Mengenal Teknologi Informasi Lebih Dekat*" dalam <http://www.kalyanamitra.or.id>

[3] Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi",* Refika Aditama, Bandung,2005, Hal.123

[4] Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya,* Laksbang Pressindo, Jogjakarta, 2007, Hal.4

4. *Cyber Espionage*
   Yaitu merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lainn, dengan cara memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen atau datanya tersimpan dalam suatu sistem yang *computeraized.*

5. *Cyber Sabotage and Extortion*
   Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program tertentu sehingga data program komputer atau sistem jaringan tidak dapat digunakan lagi, tidak berjalan sebagaimana mestinya atau berjalan sebagaimana yang dikehendaki oleh pelaku. Kejahatan ini juga sering disebut dengan kejahatan *cyber terrorism.*

6. *Offence Againts Intellectual Property*
   Kejahatan ini ditujukan terhadap HKI atau Hak kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh, meniru tampilan *web* suatu situs tertentu, penyiaran rahasia dagang yang merupakan rahasia dagang orang lain.
7. *Infringements of Privacy*
   Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan simpan secara *computerized.* Yang apabila diketahui orang lain maka dapat merupakan korban secara materiil atau immateriil, seperti nomor PIN ATM, nomor kartu kredit dan sebaginya.

Selain kejahatan yang dipaparkan diatas, terdapat juga jenis-jenis kejahatan yang masuk dalam kategori *cyber crime* yaitu:

1. *Cyber terrorism*
2. *Cyber pornography*
3. *Cyber harrassment*
4. *Cyber stalking*
5. *Hacking*
6. *Carding (credit card fraund)*

Beberapa contoh kasus *cybercrime* antara lain:

1. Pencurian dan penggunaan ***account internet*** milik orang lain yaitu: Pencurian *account* ini berbeda dengan pencurian secara fisik karena pencurian dilakukan cukup dengan menangkap "*user_id*" dan "*password*" saja. Tujuan dari pencurian itu hanya untuk mencuri informasi saja. Pihak yang kecurian tidak akan merasakan kehilangan. Namun, efeknya akan terasa jika informasi tersebut digunakan oleh pihak yang tidak bertanggung jawab. Hal tersebut akan membuat semua beban biaya penggunaan account oleh si pencuri dibebankan kepada si pemilik account yang sebenarnya. Modus kejahatan ini adalah penyalahgunaan *user_ID* dan *password* oleh seorang yang tidak punya hak.

2. Kejahatan kartu kredit yang dilakukan lewat transaksi online di Yogyakarta : Polda DI Yogyakarta menangkap lima carder dan mengamankan barang bukti bernilai puluhan juta, yang didapat dari merchant luar negeri. Begitu juga dengan yang dilakukan mahasiswa sebuah perguruan tinggi di Bandung, Buy alias Sam. Akibat perbuatannya selama setahun,

beberapa pihak di Jerman dirugikan sebesar 15.000 DM (sekitar Rp 70 juta). Para carder beberapa waktu lalu juga menyadap data kartu kredit dari dua outlet pusat perbelanjaan yang cukup terkenal. Caranya, saat kasir menggesek kartu pada waktu pembayaran, pada saat data berjalan ke bank-bank tertentu itulah data dicuri. Akibatnya, banyak laporan pemegang kartu kredit yang mendapatkan tagihan terhadap transaksi yang tidak pernah dilakukannya. Modus kejahatan ini adalah penyalahgunaan kartu kredit oleh orang yang tidak berhak.

3. Pornografi yaitu: salah satu kejahatan Internet yang melibatkan Indonesia adalah pornografi anak. Kegiatan yang termasuk pronografi adalah kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas. Motif kejahatan ini termasuk ke dalam *cybercrime* sebagai tindakan murni kejahatan. Hal ini dikarenakan para penyerang dengan sengaja membuat situs-situs pornografi yang sangat berdampak buruk terhadap masyarakat. Kejahatan kasus *cybercrime* ini dapat termasuk jenis *illegal contents*. Sasaran dari kasus kejahatan ini adalah *cybercrime* menyerang individu (*against person*).

4. Penipuan Melalui Situs Internet : Para pengguna Internet juga harus waspada dengan adanya modus penipuan lewat situs-situs yang menawarkan program-program bantuan maupun multilevel marketing (MLM). Seperti dalam program bernama *Given in Freedom Trust* (GIFT) dari sebuah situs yang tadinya beralamat di http://www.entersatu.com/danahibah. Dalam program ini, penyelenggara mengiming-imingi untuk memberikan dana hibah yang didapat dari sekelompok dermawan kaya dari beberapa negara bagi perorangan atau perusahaan, dengan syarat mengirimkan sejumlah dana tertentu ke rekening tertentu tanpa nama. Program ini menggiurkan karena untuk perorangan tiap pemohon bisa mendapat 760 dollar AS/bulan dan 3.000 dollar AS/ bulan untuk perusahaan. Kejahatan ini memiliki motif *cybercrime* sebagai tindakan murni kejahatan.

5. Penipuan Lewat Email yaitu: Penipuan lainnya dilakukan lewat surat elektronik (e-mail). Penipuan lewat media ini bahkan diindikasikan sebagai bagian dari mafia internasional. Modus operandinya, seseorang yang berasal dari luar negeri, kebanyakan dari Afrika, meminta bantuan untuk "menerima" transferan sejumlah dana dari proyek yang telah dikerjakan atau alasan lain ke rekening calon korbannya. Iming-imingnya, uang yang bernilai milyaran rupiah itu, 30 persen akan menjadi milik korban. Hanya saja, kemudian diketahui, dari beberapa laporan, mereka terlebih dahulu harus mengirimkan sekitar 0,1 persen dari dana yang akan menjadi milik korban kepada penipu tersebut. Ujungnya, setelah dikirim, uang yang dijanjikan tidak juga diterima. Kejahatan ini memiliki motif *cybercrime* sebagai tindakan murni kejahatan. Hal ini dikarenakan si pengirim dengan sengaja mengirimkan e-mail dengan maksud meminta transferan dana dengan alasan yang tidak benar.

6. Kejahatan yang berhubungan dengan nama domain yaitu: Nama domain *(domain name)* digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah cybersquatting. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain. Modus dari kegiatan kejahatan ini adalah penipuan. Motif dari kejahatan ini termasuk ke dalam *cybercrime* sebagai tindakan murni kejahatan.

7. Terjadinya perubahan dalam website KPU antara lain: Pada tanggal 17 April 2004, Dani Hermansyah melakukan *deface* dengan mengubah nama-nama partai yang ada dengan nama-nama buah dalam www.kpu.go.ig . Hal ini mengakibatkan keprcayaan masyarakat terhadap Pemilu yang sedang berlangsung pada saat itu menjadi berkurang. Dengan berubahnya nama partai di dalam website, maka bukan tidak mungkin angka-angka jumlah pemilih yang masuk di sana menjadi tidak aman dan bisa diubah. Modus dari kejahatan ini adalah mengubah tampilan *dan* informasi *website*. Motif dari kejahatan ini termasuk ke dalam *cybercrime* sebagai tindakan murni kejahatan.

8. *Denial of Service (DoS)* dan *Distributed DoS (DDos) attack y*aitu: serangan yang bertujuan untuk melumpuhkan target (*hang, crash*) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Modus dari kegiatan kejahatan ini adalah membuat tidak berfungsinya suatu servis atau layanan. Motif dari kejahatan ini termasuk ke dalam *cybercrime* sebagai tindakan murni kejahatan.

Pengaturan *Cyber Crime* didalam Hukum

Hukum yang dijadikan rujukan oleh aparat penegak hukum untuk menjaring *cyber crime* diantaranya adalah:

1. Kitab Undang-Undang Hukum Pidana (KUHP)

   Beberapa ketentuan dalam KUHP yang digunakan oleh aparat penegak hukum dalam kejahatan *cyber crime* yaitu pada pasal-pasal yang berkaitan salah satunya adalah:

   Pasal 167 yaitu:

   (1) Barangsiapa dengan melawan hak orang lain dengan memaksa kedalam rumah atau ruangan yang tertutup atau pekarangan, yang dipakai oleh orang lain, atau sedang ada disitu dengan tidak ada haknya, tidak dengan segera pergi dari tempat itu atas permintaan orang yang berhak, dihukum penjara selama-lamanya sembilan bulan atau denda sebanyak-banyaknya Rp.4500,-
   (2) Barangsiapa masuk dengan memecah atau memanjat, memakai kunci palsu, perintah palsu atau pakaian dinas palsu atau barang siapa dengan tidak setahu yang berhak dan lain daripada lantaran keliru, masuk ketempat yang tersebut tadi dan ditemukan disana pada waktu malam, dianggap sebagai sudah masuk dengan memaksa.

   Pasal 406 KUHP ayat (1) berkaitan dengan tindakan pengrusakan yang menyebutkan bahwa:

   "barangsiapa dengan sengaja dan dengan melawan hukum menghancurkan, mengrusakkan, membikin tak dapat dipakai atau menghilangkan barang sesuatu yang seluruuhnya atau sebagian adalah kepunyaan orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak tiga ratus rupiah."

   Ketentuan tersebut ditujukan (diancamkan) misalnya kepada *hacker,* karena aktivitas *hacker* ini dinilai telah menimbulkan kerusakan atau kerugian yang luar biasa kepada usaha seseorang, kepentingan institusi atau negara. Aparat menilai kalau yang dilakukan oleh *hacker* jelas-jelas mengakibatkan kerugian pada orang lain, salah satunya berupa kerusakan atau menjadikan tidak berfungsinya barang lain. Jika barang ini termasuk *website,* maka *website* inilah yang mengalami kerusakan.

   Pasal 282 KUHP

Pasal ini adalah untuk mencegah menjalarnya penggunaan jaringan internet secara melawan hukum, sebagai dasar hukum yang digunakan oleh aparat penegak hukum, yaitu sebagai berikut:

(1) Barangsiapa menyiarkan, mempertontonkan, atau menempelkan dengan terang-terangan suatu tulisan yang diketahui isinya, atau gambar atau barang yang dikenalnya melanggar perasaan kesopanan, maupun membuat, membawa masuk, mengirimkan langsung, membawa keluar atau menyediakan tulisan, gambar atau barang itu untuk disiarkan, dipertontonkan atau ditempelkan sehingga kelihatan oleh orang banyak, ataupun terang-terangan diminta atau menunjukkan bahwa tulisan, atau gambar atau barang itu boleh didapat, dihukum penjara selama-lamanya satu tahun empat bulan atau denda sebanyak-banyaknya Rp.45.000,-
(2) Barangsiapa menyiarkan, mempertontonkan atau menempelkan dengan terang-terangan suatu tulisan, gambar atau barang yang melanggar perasaan kesopanan, maupun membawa masuk, mengirimkan terus, membawa keluar atau menyediakan surat, gambar atau barang itu disiarkan, dipertontonkan atau ditempelkan, sehingga kelihatan oleh orang banyak ataupun dengan terang-terangan atau dengan menyiarkan sesuatu tulisan menawarkan dengan tidak diminta atau menunjukkan, bahwa tulisan, gambar atau barang itu tidak boleh didapat, dihukum penjara selama-lamanya sembilan bulan atau denda sebanyak-banyaknya Rp.45.000,-. Jika ada alasan yang sesungguh-sungguhnya untuk menduga, bahwa tulisan, gambar atau barang itu melanggar kesopanan.
(3) Jika melakukan kejahatan yang diterangkan dalam ayat pertama dijadikan suatu pencaharian atau kebiasaan, oleh tersangka, dapat dijatuhkan hukuman penjara selama-lamanya dua tahun delapan bulan atau denda sebanyak-banyaknya Rp.75.000,-

2. Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)
Pengaturan *cyber crime* dengan hukum pidana saat ini sudah tertuang dalam UU ITE yang berkaitan dengan masalah kriminalisasi. Ketentuan pidana mengenai kejahatan yang menggunakan transaksi elektronik ada terdapat pada BAB XI mengenai ketentuan pidana yang tertuang mulai dari pasal 45 sampai pasal 52.
Pasal 53 menyatakan bahwa

Pasal 27 Ayat (1) jo 45 Ayat (1) UU ITE

Pasal 27 Ayat (1): *Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya ITE dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.*

Ayat (2): *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 perjudian.*

Ayat (3): *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.*

Ayat (4): *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 pemerasan dan/atau pengancaman.*

Pasal 45 Ayat (1): *Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 Ayat (1), Ayat (2,) Ayat (3) atau Ayat (4) dipidana dengan pidana penjara paling lama 6 tahun dan/atau dengan paling banyak Rp 1.000.000.000,00.*

Pada saat berlakunya Undang-Undang ini, semua Peraturan Perundang-undangan dan kelembagaan yang berhubungan dengan pemanfaatan Teknologi Informasi yang tidak bertentangan dengan Undang-Undang ini dinyatakan tetap berlaku.

Solusi untuk mencega kejahatan dengan menggunakan teknologi informasi adalah sebagai berikut:

1. Pencurian dan penggunaan ***account internet*** milik orang lain solusinya adalah Penggunaan enkripsi yaitu dengan mengubah data-data yang dikirimkan sehingga tidak mudah disadap (*plaintext* diubah menjadi *chipertext*). Untuk meningkatkan keamanan authentication (pengunaan *user_id* dan *password*), penggunaan enkripsi dilakukan pada tingkat socket. Hal ini akan membuat orang tidak bias menyadap data atau transaksi yang dikirimkan dari/ke server WWW.

2. Kejahatan kartu kredit yang dilakukan lewat transaksi online di Yogyakarta solusinya adalah Perlu adanya *cyberlaw*: *Cybercrime* belum sepenuhnya terakomodasi dalam peraturan / Undang-undang yang ada, penting adanya perangkat hukum khusus mengingat karakter dari cybercrime ini berbeda dari kejahatan konvensional.

3. Pornografi solusinya adalah Di Swedia, perusahaan keamanan internet, NetClean Technology bekerjasama dengan *Swedish National Criminal Police Department* dan NGO ECPAT, mengembangkan program *software* untuk memudahkan pelaporan tentang pornografi anak. Setiap orang dapat mendownload dan menginstalnya ke computer. Ketika seseorang meragukan apakah material yang ada di internet itu legal atau tidak, orang tersebut dapat menggunakan *software* itu dan secara langsung akan segera mendapat jawaban dari ECPAT Swedia.

4. Penipuan Melalui Situs Internet solusinya adalah Meningkatkan pengetahuan dan kesadaran masyarakat tentang masalah *cybercrime* , sehingga masyarakat tidak mudah terpengaruh dengan iklan dalam situs.

5. Penipuan Lewat Email solusinya adalah Adanya kesadaran masyarakat yang sudah menjadi korban untuk melaporkan kepada polisi, sehingga korban email itu dapat dikurangi atau bahkan si pengirim email dapat segera ditangkap.

6. Kejahatan yang berhubungan dengan nama domain solusinya adalah Meningkatkan sistem pengamanan jaringan komputer nasional sesuai dengan standar internasional.

7. Terjadinya perubahan dalam website KPU solusinya adalah Penggunaan Firewall. Tujuan utama dari firewall adalah untuk menjaga agar akses dari orang tidak berwenang tidak dapat dilakukan. Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang keluar dan masuk harus melalui atau melewati firewall. Firewall bekerja dengan mengamati paker *Intenet Protocol* (IP) yang melewatinya.

8. *Denial of Service (DoS)* dan *Distributed DoS (DDos) attack* solusinya adalah Perlunya Dukungan Lembaga Khusus: Lembaga ini diperlukan untuk memberikan informasi tentang *cybercrime*, melakukan sosialisasisecara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan *cybercrime*.

Dengan adanya tulisan ini diharapkan para pembaca nantinya akan paham dan mengerti apabila menggunakan internet dan untuk menyimpan kerahasiaan data yang kita punya agar lebih hati-hati dalam menggunakan internet dan juga nantinya mengerti bagaimana apabila *cyber crime* terjadi dengan kita. Sejauh apa undang-undang kita mengatur mengenai kejahatan tersebut.

BAHAN BACAAN

Abdul Wahid dan M. Labib, "*Kejahatan Mayantara (Cyber Crime)",* Refika Aditama, Bandung, 2005

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi",* Refika Aditama, Bandung,2005

Kitab Undang-Undang Hukum Pidana (KUHP)

Sulistyo Basuki "*Mengenal Teknologi Informasi Lebih Dekat*" dalam http://www.kalyanamitra.or.id

Sutarman, *Cyber Crime Modus Operandi dan Penanggulangannya,* Laksbang Pressindo, Jogjakarta, 2007

Undang-Undang Informasi dan Teknologi Informasi (UU ITE)