DOS ATTACK SEBAGAI TINDAK PIDANA SIBER DALAM PENGATURAN HUKUM DI INDONESIA

Cheny Berlian

Universitas Muhammadiyah Riau, Indonesia, chenyberlian@umri.ac.id

Abstract

Denial of Service (DoS) Attack is an attack that aims to disable the target (hang, crash) so that it cannot provide services. This attack does not steal, eavesdrop, or falsify data, but with the loss of service, the target does not provide services so there is a financial loss. Because DoS Attacks can attack the system of a bank and damage it, so that customer data on the bank's server will be lost. Based on the background the author describes above, in this study the author formulates the main problem as follows: How does DOS Attack Existence as a Criminal Act in Indonesian Law Arrangements? This research, when viewed from its type, is classified as normative legal research by using a normative juridical approach, namely by reviewing the relevant literature, the opinions of related legal experts and analyzing cases in documents, such as by analyzing journals related to DoS. This attack is to clarify the research results. According to the results of the research that the author did, DoS Attack at this time has become a very dangerous threat and needs more intensive supervision. Because now there are many DoS Attacks that are detrimental to many parties, such as the government with the occurrence of attacks on the KPU website to the destruction of the banking system owned by banks.

Keyword: *Criminal, DOS, Cyberlaw*

Abstrak

Denial of Service (DoS) Attack merupakan serangan yang bertujuan untuk melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data, akan tetapi dengan hilangnya pelayanan maka target tidak memberikan servis sehingga ada kerugian finansial. Karena DoS Attack dapat menyerang sistem dari suatu bank dan merusaknya, sehingga data-data milik nasabah yang ada di dalam dalam server milik bank tersebut akan hilang. Berdasarkan latar belakang penulis jabarkan di atas, maka dalam penelitian ini penulis merumuskan masalah pokok sebagai berikut: Bagaimanakah Eksistensi DOS Attack Sebagai Tindak Pidana Dalam pengaturan Hukum di Indonesia Penelitian ini jika dilihat dari jenisnya maka tergolong sebagai penelitian *hukum normatif* dengan cara menggunakan pendekatan yuridis normatif yaitu dengan mengkaji literatur-literatur yang berkaitan, pendapat para ahli-ahli hukum terkait dan analisa kasus dalam dokumen-dokumen, seperti dengan menganilis jurnal yang berhubungan dengan DoS Attack ini untuk memperjelas hasil penelitian. Menurut hasil penelitian yang penulis lakukan bahwa DoS Attack pada saat ini sudah menjadi ancaman yang sangat berbahaya dan perlu pengawasan lebih intensif. Karena sekarang banyaknya terjadi DoS Attack yang merugikan banyak pihak, seperti pemerintah dengan terjadinya kasus penyerangan situs KPU hingga pengrusakan sistem perbankan yang dimiliki oleh bank.

Kata Kunci: Kriminal, DOS, Hukum Siber

Pendahuluan

Perkembangan teknologi informasi pada saat ini sangat cepat dan jauh berbeda pada masa awal kehadirannya. Era globalisasi telah menempatkan peranan teknologi informasi ke dalam suatu posisi yang sangat strategis karena dapat menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu serta dapat meningkatkan produktivitas serta efisiensi. Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung secara cepat dengan signifikan.

Pemanfaatan media internet pada masa sekarang ini memberikan dampak yang cukup luas bagi hampir sebagian besar aspek kehidupan manusia dimana internet menjadi media penyampaian serta pertukaran informasi, disamping juga sebagai sarana atau media baru dalam melakukan interaksi sosial yang biasanya terjadi secara tidak langsung dan bersifat *borderless* (tanpa mengenal batas wilayah).

Masyarakat itu sendirilah yang melahirkan suatu kejahatan. Semakin tinggi tingkat intelektualitas suatu masyarakat, semakin canggih pula kejahatan yang mungkin terjadi dalam masyarakat itu.[1]

Menurut E.A Hobel sebagaimana yang dikutip oleh Lili Rasjidi, mengatakan bahwa hukum mempunyai fungsi yang sangat penting yaitu menjaga keutuhan masyarakat. Adapun fungsi-fungsi hukum tersebut adalah:

1. Menetapkan hubungan mana yang boleh dilakukan oleh anggota-anggota masyarakat, dan hubungan mana yang tidak boleh dilakukan.
2. Menentukan alokasi wewenang, dan menentukan secara seksama badan-badan mana yang berwenang melakukan paksaan, dengan sekaligus menentukan sanksi-sanksi mana yang dianggap tepat dan efektif.
3. Disposisi masalah-masalah sengketa.

[1] http://olahfikir.wordpress.com/2012/10/09/cyber-crime-kejahatan-di-dunia-maya/ diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

4. Menyesuaikan pola-pola hubungan dengan perubahan dalam masyarakat.[2]

Tumbuh dan berkembangnya teknologi komputer, teknologi informasi, dan teknologi komunikasi telah menyebabkan munculnya berbagai macam jenis tindak pidana baru yang memiliki karakteristik berbeda dengan tindak pidana biasa yang selama ini dikenal di masyarakat dan telah diakomodir di dalam KUHP (Kitab Undang-undang Hukum Pidana).

Dalam perkembangannya teknologi informasi tidak hanya memberikan dampak positif, seperti kemudahan dalam melakukan jual beli barang (*online shop*) ataupun kemudahan dalam pencarian data informasi yang diinginkan, akan tetapi teknologi informasi juga menyebabkan timbulnya jenis kejahatan baru, yaitu kejahatan yang berbeda dengan kejahatan konvesional. Berbeda dengan kejahatan konvensional, dimana pelaku tindak kejahatan harus melakukan kontak fisik dengan korbannya, seperti pencurian, dalam kejahatan mayantara (*cybercrime*) pelaku tindak kejahatan dapat melancarkan aksinya kepada korban tanpa perlu bersusah payah harus melakukan kontak fisik pada korban tersebut.

Ada banyak jenis *cybercrime* yang ada di Indonesia yaitu *hacking, cracking, defacing, carding, fraud, spamming, cyberpornography,* dan *online gambling*. Berdasarkan banyaknya jenis *cybercrime* tersebut ada yang bernama Denial of Service (DoS) Attack, yang mana DoS Attack ini merupakan bentuk akhir dari tindakan *cracking*, yang mana mempunyai dampak yang sangat buruk terhadap suatu sistem.

Cracking adalah proses bagaimana seseorang menyusup ke dalam sistem milik orang lain, dengan tujuan untuk merusak sistem tersebut, orang yang melakukan *cracking* disebut *cracker*.[3] Sebaliknya *Hacking* adalah bagaimana seseorang menyusup ke dalam sistem

[2] Lili Rasjidi, *Dasar-Dasar Filsafat dan Teori Hukum*, Citra Aditya Bakti, Bandung, 2001, hlm. 21.

[3] Efvy Zam, *Buku Sakti Hacker*, Mediakita, Jakarta, 2011, hlm. 1.

milik orang lain, tetapi tidak merusak sistem tersebut. Dan orang yang melakukan *Hacking* disebut dengan *Hacker*.[4]

Denial of Service (DoS) Attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data, akan tetapi dengan hilangnya pelayanan maka target tidak memberikan servis sehingga ada kerugian finansial.[5] Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi, akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS Attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan *bandwidth*).

Adapun Pasal-pasal yang dilanggar oleh pelaku DoS Attack berdasarkan Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, antara lain:

1) Pasal 31 ayat (2), berbunyi.

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

"Sanksi yang akan didapat tertera pada Pasal 47, yang berbunyi " Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 sepuluh) tahun dan/atau

[4] *Ibid.*
[5] *Ibid.*, hlm. 319.

denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).”[6]

2) Pasal 32 ayat (1), berbunyi.

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.”

Sanksi yang akan didapat tertera pada Pasal 48 ayat 1, yang berbunyi “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.000,00(dua miliar rupiah).”[7]

3) Pasal 33, berbunyi.

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.”

Sanksi yang akan didapat tertera pada Pasal 49, yang berbunyi “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00(sepuluh miliar rupiah).”[8]

4) Pasal 36, berbunyi.

“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.”

“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda

[6] O.C Kaligis, *Penerapan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi & Transaksi Elektronik Dalam Prakteknya*, Yarsif Watampone, Jakarta, 2012, hlm. 562.
[7] *Ibid.* hlm. 563.
[8] *Ibid.*

paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).”[9]

Adapun berita terkait Kasus DoS Attack yang pernah terjadi di Indonesia, yaitu kasus terkait ulah *cracker* yang merusak sistem jaringan Facebook.

Dikutip dari Koran tempo 3 Desember 2009:

“Serangan DoS Memperlambat Akses Facebook”


INDONESIA ENGLISH

TEMPO.CO

tekno

KAMIS, 31 OKTOBER 2013 | 00:21 WIB ENGLISH EDITION MAJALAH TEMPO KORAN TEMPO TRAVELOUN

Bisnis | Bola | Gaya! | Dunia | Metro | Politik | Olahraga | Otom

Home ▶ Tekno ▶ It

KAMIS, 03 DESEMBER 2009 | 19:31 WIB

Serangan DOS Memperlambat Akses Facebook

Follow 411K followers Suka 231r

+ Besar – Kecil A Normal

TEMPO *Interaktif*, Jakarta - Serangan Denial of Service (DOS) ditengarai memperlambat koneksi jaringan operator jejaring sosial dan pencari data di internet, seiring tingginya jumlah pengguna jasa layanan seperti Facebook, Yahoo!, Google, Twitter.

"Kecepatan akses data yang tidak sesuai harapan kemungkinan karena serangan `Denial of Services/DOS` dari penyusup atau virus, sehingga berakibat kinerja layanan drop," kata Kepala Laboratorium Komputasi Berbasis Jaringan, Jurusan Teknik Informatika, FTIF Institut Teknologi Sepuluh November Surabaya (ITS), M. Husni, Selasa.

Menurut dia, biasanya waktu yang diperlukan untuk memperbaiki lemahnya akses tersebut tidak sampai 12 jam. "Perbaikan selama itu

Berita T

Lima Hacke

Waspada S Steve Jobs

Komputer M bulanan Viru

Akun Faceb Mahasiswi L

Gawat, 1 da Pelecehan S Internet

Grafis T

Gambar I.1 Serangan DoS Memperlambat Akses Facebook.

TEMPO Interaktif, Jakarta – Serangan Denial of Service (DoS) ditengarai memperlambat koneksi jaringan operator jejaringan sosial dan pencari data di internet, seiring tingginya jumlah pengguna jasa layanan seperti Facebook, Yahoo!, Google, Twitter. “Kecepatan akses data yang tidak sesuai harapan kemungkinan karena serangan `Denial of Service/DoS` dari penyusup atau virus, sehingga berakibat kinerja layanan drop, ”kata Kepala Laboratorium Komputasi Berbasis Jaringan”, Jurusan Teknik Informatika, FTIF Institut Teknologi Sepuluh November Surabaya (ITS), M.Husni, Selasa.

Menurut dia, biasanya waktu yang diperlukan untuk memperbaiki lemahnya akses tersebut tidak sampai 12 jam. “Perbaikan selama itu mengingat tenaga Teknologi Informasi harus menganalisis dan melakukan `scanning` terhadap semua `port`,” Ujarnya. Tapi tak usah khawatir, pada umumnya data-data yang disimpan di sejumlah operator seperti Facebook, Yahoo!, Google, Twitter, cukup aman atau tidak hilang, bahkan ada kemungkinan operator tersebut menggunakannya untuk keperluan sendiri.[10]

Berdasarkan berita tersebut penulis memahami perlunya Undang-undang yang mengatur hal terkait kejahatan mayantara, maka pada Tahun 2008 disahkanlah Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[9] *Ibid.* hlm. 564.

[10] http://www.tempo.co/read/news/2009/12/03/072211766/Serangan-DOS-Memperlambat-Akses-Facebook diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

Tidak hanya polisi bahkan masyarakat pun menyambut baik kehadiran undang-undang yang khusus mengatur mengenai *cyber crime* ini. Terlebih lagi dengan adanya pengaturan yang khusus mengenai transaksi elektronik, yang diharapkan dapat mengatasi Bentuk-bentuk tindak pidana seperti *credit card fraud* (penipuan melalui kartu kredit), *hacking*, dan lain-lain. Dahulu kasus-kasus semacam ini, yang mulai melanda Indonesia, boleh dikatakan hampir tidak tersentuh oleh hukum. Sehingga pihak yang berwenang tidak mempunyai dasar hukum yang pasti untuk menangani *cyber crime* yang masih samar. Dengan demikian *cyber crime* ini kemungkinan besar tidak bisa diajukan ke meja hijau. Tetapi keadaan seperti itu sudah tidak berlaku lagi karena sekarang telah disahkan Undang-Undang tentang Informasi dan Transaksi Elektronik.

Onno W. Purbo, ahli TI dari Institut Teknologi Bandung, menjelaskan bahwa bentuk-bentuk *cyber crime*, antara lain penipuan kartu kredit (disebut juga dengan *carding)* dan merusak website milik orang lain. 4 Contoh *cyber crime* lainnya, menurut *Yuyun Mulyana* (Asisten Bimmas Polri), di antaranya adalah akses secara tidak sah, pelanggaran Hak Kekayaan Intelektual (HaKI), penghinaan dan sebagainya. Barda Nawawi Arief, memberikan istilah lain mengenai *cyber crime* semacam ini dengan istilah tindak pidana dunia maya.[11]

Praktik tindak pidana dunia maya juga menyebabkan dunia bisnis nasional harus mengalami dampak kerugian besar, sebagai contoh adanya kasus-kasus seperti pemalsuan nama *website* layanan *internet banking* Bank BCA dan perebutan nama *domain website* milik perusahaan Mustika Ratu yang sempat mencuat menjadi kasus tindak pidana internet nasional beberapa waktu lalu.

Menurut Judith M.S ketua presidium Asosiasi Warnet Indonesia, *cyber crime* dalam bentuk *carding* atau *credit card fraud*

[11] Onno W. Purbo, *Filosofi Naif Kehidupan Dunia Cyber*, Republika, Jakarta, 2003, hlm. 18.

(penipuan melalui kartu kredit) adalah Tindak pidana internet yang paling meresahkan di Indonesia sekarang ini. Penipuan tersebut dilakukan dengan cara menggunakan nomor rekening kartu kredit milik orang lain untuk melakukan pembayaran dengan dana yang ada pada kartu kredit tersebut tanpa seizin pemilik sah kartu kredit atas transaksi melalui media internet.[12]

Pemecahannya yang paling utama diperlukan adalah adanya perangkat hukum atau peraturan perundang-undangan yang jelas. Perlunya perangkat hukum ini, diakui oleh aparat hukum sendiri. Dengan disahkannya Undang-Undang tentang Informasi dan Transaksi Elektronik, maka diharapkan Undang-undang ini dapat menjadi solusi atas permasalahan yang selama ini dialami Indonesia mengenai penanganan tindak pidana dunia maya ini.

Penanganan kasus yang terjadi sebelum Undang-Undang tentang Informasi dan Transaksi Elektronik ini disahkan adalah dengan cara melakukan analogi terhadap pasal-pasal yang terdapat di dalam Kitab Undang-Undang Hukum Pidana yang paralel dengan tindak pidana yang terjadi. Sehingga para penjahat dunia maya pun dipidana dengan Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP).

Saat ini walaupun pada hakikatnya setiap orang yang melakukan tindak pidana mayantara akan dikenai sanksi berdasarkan UU No.11 tentang ITE, tetapi sepertinya hal tersebut belum dapat diterapkan dengan baik. Banyak terjadinya tindak pidana mayantara yang terjadi, namun pihak berwajib belum dapat menjalankan perannya dengan baik dalam mengusut dan menyelesaikan kasus-kasus *cybercrime* yang terjadi di Indonesia. DoS Attack yang sering terjadi terhadap website-website milik pemerintah dalam negeri maupun milik pihak swasta, tidak dapat diusut dengan baik, padahal kerugian

[12] http://groups.yahoo.com/group/asosiasi-warnet/message/106831 diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

finansial yang ditimbulkan oleh pelaku DoS Attack itu tidaklah sedikit.

Berdasarkan uraian di atas penulis tertarik untuk mengadakan penelitian dan mengkaji mengenai kejahatan di dunia maya (*cybercrime*) dan menelaahnya lebih jauh dalam jurnal yang berjudul **"DOS ATTACK SEBAGAI TINDAK PIDANA SIBER DALAM PENGATURAN HUKUM DI INDONESIA".**

Rumusan Masalah

Berdasarkan latar belakang masalah yang penulis uraikan di atas, maka penulis tertarik untuk meneliti terkait kajian Bagaimanakah Eksistensi DOS Attack Sebagai Tindak Pidana Dalam pengaturan Hukum di Indonesia

Tujuan Penelitian

Tujuan utama yang hendak dicapai dalam penelitian ini adalah untuk memperoleh pemahaman secara mendalam untuk mengetahui Bagaimanakah Eksistensi DOS Attack Sebagai Tindak Pidana Dalam pengaturan Hukum di Indonesia

Metode Penelitian

Untuk menghasilkan penelitian secara baik dan berkualitas sesuai dengan standar keilmiahan, maka penulis menggunakan metode penelitian hukum normatif, dan sifat penelitian ini deskriptif analisis. Penelitian ini menggunakan berbagai sumber, seperti, buku, website yang berkaitan dengan DoS Attack. Kemudian penulis menarik kesimpulan dari setiap sumber dan membuatnya menjadi sebuah karya ilmiah yang baik. Hasil penelitian ini tidak bersifat valid, karena tujuannya bukan untuk membentuk teori, melainkan menguji teori yang telah ada dalam situasi sebenarnya.

Hasil dan Pembahasan

Pada saat ini eksistensi DoS sudah cukup dikenal oleh masyarakat Indonesia, berdasarkan cukup banyaknya kasus-kasus yang terjadi, dan berikut ini adalah

beberapa contoh kasus-kasus DoS Attack yang pernah terjadi.

Contoh kasus-kasus DoS Attack yang pernah terjadi adalah:

1. 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. Hal ini dikarenakan para penyerang dengan sengaja mengubah tampilan dan informasi dari website. Kejahatan kasus *cybercrime* ini dapat termasuk jenis *hacking* dan *cracking*, *data frogery*, dan bisa juga cyber terorism. Sasaran dari kasus kejahatan ini adalah cybercrime menyerang hak milik (*against property*) dan bisa juga cybercrime menyerang pemerintah (*against government*).[13]
2. *Amazon*, *eBay*, *CNN*, dan *Yahoo!* Ada awal Februari 2000, sebuah serangan yang besar dilakukan sehingga beberapa situs web terkenal seperti *Amazon, CNN, eBay, dan Yahoo!* mengalami "downtime" selama beberapa jam. Serangan yang lebih baru lagi pernah dilancarkan pada bulan Oktober 2002 ketika 9 dari 13 *root DNS Server* diserang dengan menggunakan DoS yang sangat besar yang disebut dengan "*Ping Flood*". Pada puncak serangan, beberapa server tersebut pada tiap detiknya mendapatkan lebih dari 150.000 request paket *Internet Control Message Protocol* (ICMP). Untungnya,

[13] http://ourcreated.blogspot.com/2012/05/contoh-kasus-cybercrime-yang-terjadi-di.html diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

karena serangan hanya dilakukan selama setengah jam saja, lalu lintas Internet pun tidak terlalu terpengaruh dengan serangan tersebut (setidaknya tidak semuanya mengalami kerusakan).[14]

3. Juli 2008, banyak blog milik blogger-blogger konservatif, termasuk Macsmind.com, merasa mendapat serangan DoS attack hingga beberapa terpaksa harus offline. Serangan ini dikaitkan dengan 3 IP address yang diregister melalui GoDaddy.com ke barrackobama.com, situs resmi calon presiden AS dari partai Demokrat, Barrack Obama. Sebelumnya, beberapa pendukung Obama juga melakukan serangan ke situs-situs pendukung Hillary Rodham Clinton dengan menggunakan google.com. Sampai 8 Agustus kemarin, asal pasti serangan masih belum jelas, namun Obama atau tim kampanyenya secara personal dianggap terlibat.[15]
4. Dikutip dari Koran tempo 3 Desember 2009:

   "Serangan DoS Memperlambat Akses Facebook"

   TEMPO Interaktif, Jakarta – Serangan Denial of Service (DoS) ditengarai memperlambat koneksi jaringan operator jejaringan sosial dan pencari data di internet, seiring tingginya jumlah pengguna jasa layanan seperti Facebook, Yahoo!, Google, Twitter. "Kecepatan akses data yang tidak sesuai harapan kemungkinan karena serangan `Denia of Service/DoS` dari penyusup atau virus, sehingga berakibat kinerja layanan drop, "kata Kepala Laboratorium Komputasi Berbasis Jaringan", Jurusan Teknik Informatika, FTIF Institut Teknologi Sepuluh November Surabaya (ITS), M.Husni, Selasa.

[14] http://rydevsan.wordpress.com/2013/04/23/cyber-crime-di-indonesia/ diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

[15] http://kacrut-team.blogspot.com/2013/04/contoh-kasus.html diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

Menurut dia, biasanya waktu yang diperlukan untuk memperbaiki lemahnya akses tersebut tidak sampai 12 jam. "Perbaikan selama itu mengingat tenaga Teknologi Informasi harus menganalisis dan melakukan `scanning` terhadap semua `port`," Ujarnya. Tapi tak usah khawatir, pada umumnya data-data yang disimpan di sejumlah operator seperti Facebook, Yahoo!, Google, Twitter, cukup aman atau tidak hilang, bahkan ada kemungkinan operator tersebut menggunakannya untuk keperluan sendiri.[16]

Itulah beberapa contoh kasus-kasus DoS Attack yang pernah terjadi, dan berdasarkan kasus-kasus tersebut dapat dilihat bahwa pelaku tindak pidana mayantara tersebut telah melanggar UU No.11 Tahun 2008 Tentang ITE, yang akan dijabarkan berikut:

"Undang–undang Cyber Mengenai Denial of Service Attack"

Beberapa Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Yang Berhubungan dengan Denial of Service Attack antara lain:

1) Pasal 31 ayat (2), berbunyi

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
> "Sanksi yang akan didapat tertera pada Pasal 47, yang berbunyi " Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 sepuluh) tahun dan/atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah)."[17]

2) Pasal 32 ayat (1), berbunyi

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan

[16] http://www.tempo.co/read/news/2009/12/03/072211766/Serangan-DOS-Memperlambat-Akses-Facebook diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

[17] O.C Kaligis, *Penerapan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi & Transaksi Elektronik Dalam Prakteknya*, Yarsif Watampone, Jakarta, 2012, hlm.562

cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik."
Sanksi yang akan didapat tertera pada Pasal 48 ayat 1, yang berbunyi "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp 2.000.000.000,00(dua miliar rupiah)."[18]

3) Pasal 33, berbunyi

"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya."
Sanksi yang akan didapat tertera pada Pasal 49, yang berbunyi "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00(sepuluh miliar rupiah)."[19]

4) Pasal 36, berbunyi

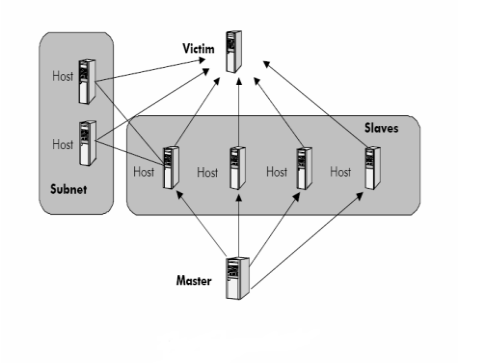
"Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain."
"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)."[20]

a. Klasifikasi DoS Attack

Denial Of Service Attack adalah serangan yang paling sering digunakan daripada serangan yang lain, hal ini dikarenakan mudahnya untuk melakukannya, exploits-nya pun banyak ditemukan di internet. Siapapun bisa men-down kan sebuah website dengan hanya menggunakan simple command prompt. Tujuan utama serangan ini adalah membuat suatu sistem crash & karena overload sehingga tidak bisa diakses atau mematikan service.[21]

Sebagaimana gambar yang ditunjukkan di bawah ini, serangan-serangan dikelompokkan menjadi tiga komponen : computer master, korban dan sejumlah komputer slave.

[18] *Ibid,* hlm .563.
[19] *Ibid*.
[20] *Ibid*., hlm. 564.
[21] Evfy Zam.,*op. cit.*, hlm. 319.



Gambar III.1 Denial of Service Attack

Gambar di atas menunjukkan bahwa penyerang mampu untuk mengambil alih sejumlah server yang disebut *slave*, dan penyerang menggunakan slave-slave tersebut untuk mengambil melancarkan serangan terhadap korban, para slave diperintahkan oleh server penyerang yang disebut master, dalam sejumlah kasus, slave sesungguhnya menggunakan host lainnya dalam subnet yang terdapat dalam jaringannya untuk melancarkan makin banyak trafik ke korban. Sebelum melancarkan serangan, penyerang masuk ke dalam sejumlah host, biasanya server besar dengan bandwidth yang besar dan menginstal slave-slave software yang menunggu perintah dari computer master untuk mengirim request ke situs korban. Begitu software tersebut diinstal pada computer slave penyerang bebas untuk menyerang situs yang mana saja. Penyerang dapat menggunakan IP address spoofing (IP address palsu) untuk menyembunyikan diri.

Berikut adalah beberapa Klasifikasi Dos Attack:

1) *Land Attack*

Land attack merupakan serangan kepada sistem dengan menggunakan program yang bernama *"land".* Program land menyerang server yang dituju dengan mengirimkan packet palsu yang seolah-olah berasal dari server yang dituju. Dengan kata lain, source dan destination dari packet dibuat seakan-akan berasal dari server yang dituju. Akibatnya server yang diserang menjadi bingung.

2) *Latierra*

Program *latierra* merupakan "perbaikan" dari program land, dimana port yang digunakan berubah-ubah sehingga menyulitkan bagi pengamanan.

3) *Ping Broadcast (smurf)*

Salah satu mekanisme serangan yang baru-baru ini mulai marak digunakan adalah menggunakan ping ke alamat *broadcast*, ini yang sering disebut dengan *smurf.* Seluruh komputer *(device)* yang berada di alamat broadcast tersebut akan menjawab. Jika sebuah sistem memiliki banyak komputer *(device)* dan ping broadcast ini dilakukan terus menerus, jaringan dapat dipenuhi oleh respon-respon dari device-device tersebut. Akibatnya jaringan menjadi lambat.

4) *Ping of Death (PoD)*

Ping-o-death sebetulnya adalah eksploitasi program *ping* dengan memberikan packet yang ukurannya besar ke sistem yang dituju. Beberapa sistem UNIX ternyata menjadi hang ketika diserang dengan cara ini. Program ping umum terdapat di berbagai operating system, meskipun umumnya program ping tersebut mengirimkan packet dengan ukuran kecil (tertentu) dan tidak memiliki fasilitas untuk mengubah besarnya packet. Salah satu implementasi program ping yang dapat digunakan untuk mengubah ukuran packet adalah program ping yang ada di sistem Windows 95.[22]

b. Karakteristik DoS Attack

Dos Attack ditandai oleh usaha attacker untuk mencegah legitimate user penggunaan resource yang diinginkan. Cara DoS Attack:

1) Mencoba untuk membanjiri (*flood*) *network*, dengan demikian mencegah lalu lintas yang legitimate pada network.

---

[22] http://eptikdws10.wordpress.com/2012/11/13/denial-of-servicedos-attack/ diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

2) Mencoba mengganggu koneksi antara dua mesin, dengan demikian mencegah suatu akses layanan.
3) Mencoba untuk mencegah individu tertentu dari mengakses layanan.
4) Mencoba untuk mengganggu layanan sistem yang spesifik atau layanan itu sendiri.[23]

c. Akibat dari DoS Attack

Denial of Service Attack mempunyai dampak yang sangat buruk terhadap perangkat maupun jaringan pada komputer, akibat-akibat dari DoS Attack adalah sebagai berikut:[24]

1) Korban *Hang*

Pada keadaan ini korban tidak bisa dioperasikan. Ditandai saat sedang ingin menggerakkan mouse, mouse tidak bergerak. Ketika mengetik pada keyboard, komputer tidak merespon. Tetapi apabila serangan tersebut dihentikan maka server dapat dioperasikan kembali.

2) Korban *Crash*

Pada keadaan ini korban mengalami *karnel panic,* yaitu keadaan yang membuat sebuah karnel sistem operasi error. Pada layar korban akan muncul tulisan karnel panic. Jika hal ini terjadi, korban tidak bisa merespon semua perintah walaupun DoS Attack telah berhenti dilakukan. Solusinya korban harus me-restart komputernya kembali.

3) Kerusakan Secara Permanent.

Serangan DoS attack yang handal akan membuat korban mengalami kerusakan pada sistem software ataupun hardware secara permanen. Hal ini bisa membuat administrator frustasi karena mau tidak mau harus mengkonfigurasi ulang

[23] http://jobtocampus.blogspot.com/2012/11/tentang-denial-of-service.html diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

[24] http://rydevsan.wordpress.com/2013/04/23/cyber-crime-di-indonesia/ diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

sistem software atau hardware agar dapat berfungsi dengan normal kembali.

4) Service Macet

Pada waktu korban mendapat serangan DoS attack, dalam keadaan sesaat ketika DoS attack terjadi, korban tidak akan bisa memberikan service.

d. Tools DoS Attack

Dalam menjalankan aksinya para pelaku DoS Attack menggunakan berbagai Tools, adapun Tools tersebut adalah sebagai berikut :

1) KOD (*Kiss Of Death*)

Merupakan tool Denial of Service yang dapat digunakan untuk menyerang Ms.Windows pada port 139 (port netbios-ssn). Fungsi utama dari tool ini adalah membuat hang/blue screen of death pada komputer korban.

2) BONK

BONK adalah dasar dari teardrop (teardrop.c). Bonk merupakan tool yang dapat membuat crash mesin MS.Windows 9x dan NT.

3) Jolt

Jolt sangat ampuh sekali untuk membekukan Windows 9x dan NT. Cara kerja Jolt yaitu mengirimkan serangkaian series of spoofed dan fragmented ICMP Packet yang tinggi sekali kepada korban.

4) NesTea

Tool ini dapat membekukan Linux dengan Versi kernel 2.0.kebawah dan Windows versi awal. Versi Improve dari NesTea dikenal dengan NesTea2.

5) NewTear

Merupakan varian dari teardrop (teardrop.c) namun berbeda dengan bonk (bonk.c).

6) Syndrop

Merupakan serangan gabungan dari TearDrop dan TCP SYN

Flooding. Target serangan adalah Linux dan Windows.

7) TearDrop

TearDrop Mengirimkan paket Fragmented IP ke komputer (Windows) yang terhubung ke jaringan (network). Serangan ini memanfaatkan overlapping ip fragment, bug yang terdapat pada Windows 9x dan NT. Dampak yang timbul dari serangan ini adalah Blue Screen of Death.

e. Langkah-langkah untuk menanggulangi DoS Attack.

Adapun langkah-langkah dalam menanggulangi DoS Attack adalah sebagai berikut:

1) Memakai Enjurnal

Enkripsi adalah ukuran security yang pertama, tetapi banyak wireless access points (WAPs) tidak menggunakan enkripsi sebagai defaultnya. Meskipun banyak WAP telah memiliki Wired Equivalent Privacy (WEP) protocol, tetapi secara default tidak diaktifkan. WEP memang mempunyai beberapa lubang di securitynya, dan seorang hacker yang berpengalaman pasti dapat membukanya, tetapi itu masih tetap lebih baik daripada tidak ada enkripsi sama sekali. Pastikan untuk men-set metode WEP authentication dengan "shared key" daripada "open system". Untuk "open system", dia tidak mengencrypt data, tetapi hanya melakukan otentifikasi client. Ubah WEP key sesering mungkin, dan pakai 128-bit WEP dibandingkan dengan yang 40-bit.

2) Gunakan Enjurnal yang kuat

Karena kelemahan kelemahan yang ada di WEP, maka dianjurkan untuk menggunakan Wi-Fi Protected Access (WPA) juga. Untuk memakai WPA, WAP harus mensupportnya. Sisi client juga harus dapat men-support WPA tersebut.

3) Ganti Default Password Administrator.

Default password umumnya sudah diketahui oleh para hacker, yang nantinya dapat menggunakannya untuk merubah

setting di WAP anda. Hal pertama yang harus dilakukan dalam konfigurasi WAP adalah mengganti password default tersebut. Gunakan paling tidak 8 karakter, kombinasi antara huruf dan angka, dan tidak menggunakan kata-kata yang ada dalam kamus.

4) Matikan SSID Broadcasting.

Service Set Identifier (SSID) adalah nama dari wireless network kita. Secara default, SSID dari WAP akan di broadcast. Hal ini akan membuat user mudah untuk menemukan network tersebut, karena SSID akan muncul dalam daftar available networks yang ada pada wireless client. Jika SSID dimatikan, user harus mengetahui lebih dahulu SSID-nya agar dapat terkoneksi dengan network tersebut.

5) Matikan WAP saat tidak di pakai.

Jika kita mempunyai user yang hanya terkoneksi pada saat-saat tertentu saja, tidak ada alasan untuk menjalankan wireless network setiap saat dan menyediakan kesempatan bagi intruder untuk melaksanakan niat jahatnya. Kita dapat mematikan access point pada saat tidak dipakai. Info: GSM fax machine, wireless CDMA, wireless GSM, fax machine.

6) Ubah Default SSID

Pabrik menyediakan default SSID. Kegunaan dari mematikan broadcast SSID adalah untuk mencegah orang lain tahu nama dari network kita, tetapi jika masih memakai default SSID, tidak akan sulit untuk menerka SSID dari network kita.

7) Memakai MAC Filtering.

Kebanyakan WAP (bukan yang murah-murah tentunya) akan memperbolehkan kita memakai filter media access control (MAC). Ini artinya kita dapat membuat “white list” dari computer-computer yang boleh mengakses wireless network kita, berdasarkan dari MAC atau alamat fisik yang ada di network card masing-masing pc. Koneksi dari MAC yang tidak ada dalam list akan ditolak.

8) Mengisolasi wireless network dari LAN.

Untuk memproteksi internal network kabel dari ancaman yang datang dari wireless network, perlu kiranya dibuat wireless DMZ atau perimeter network yang mengisolasi dari LAN. Artinya adalah memasang firewall antara wireless network dan LAN.

Dan untuk wireless client yang membutuhkan akses ke internal network, dia haruslah melakukan otentifikasi dahulu dengan RAS server atau menggunakan VPN. Hal ini menyediakan extra layer untuk proteksi. Tentunya ada perbedaan antara wireless CDMA dengan wireless GSM.

9) Mengontrol signal wireless.

802.11b WAP memancarkan gelombang sampai dengan kira kira 300 feet. Tetapi jarak ini dapat ditambahkan dengan cara mengganti antenna dengan yang lebih bagus. Dengan memakai high gain antena, kita bisa mendapatkan jarak yang lebih jauh. Directional antenna akan memancarkan sinyal ke arah tertentu, dan pancarannya tidak melingkar seperti yang terjadi di antenna omnidirectional yang biasanya terdapat pada paket WAP standard. Info: GSM fax machine - fax machine.

10) Memancarkan gelombang pada frekuensi yang berbeda.

Salah satu cara untuk bersembunyi dari hacker yang biasanya memakai teknologi 802.11b/g yang lebih populer adalah dengan memakai 802.11a. Karena 802.11a bekerja pada frekuensi yang berbeda (yaitu di frekuensi 5 GHz), NIC yang di desain untuk bekerja pada teknologi yang populer tidak akan dapat menangkap sinyal tersebut.[25]

Pada saat ini Eksistensi DoS Attack dan Tindak Pidana Mayantara lainnya menjadi sebuah pertanyaan bagi khalayak banyak, terkait bagaimana Hukum Pidana Indonesia mengaplikasikannya pada saat sekarang ini.

a. Kebijakan Formulasi Hukum Pidana Terhadap Tindak Pidana Teknologi Informasi Saat Ini.

[25] http://odydamora.blogspot.com/2009/10/denial-of-service-attack-pada-wireless.htmld diakses tanggal 26 Mei 2022, pukul 19.00 WIB.

Globalisasi teknologi informasi yang telah mengubah dunia ke era *cyber* dengan sarana internet yang menghadirkan *cyberspace* dengan realitas virtualnya menawarkan kepada manusia berbagai harapan dan kemudahan. Akan tetapi di balik itu, timbul persoalan berupa kejahatan yang dinamakan *cybercrime*, baik sistem jaringan komputernya itu sendiri yang menjadi sasaran maupun komputer itu sendiri yang menjadi sarana untuk melakukan kejahatan. Tentunya jika kita melihat bahwa informasi itu sendiri telah menjadi komoditi maka upaya untuk melindungi asset tersebut sangat diperlukan.

Kebijakan sebagai upaya untuk melindungi informasi membutuhkan suatu pengkajian yang sangat mendalam, menyangkut aspek sosiologis, filosofis, yuridis, dan sebagainya. Teknologi informasi sekarang ini sangat strategis dan berdampak luas terhadap aktifitas kehidupan manusia oleh karena itu dibutuhkan pengaturan secara khusus dengan dibentuknya suatu undang-undang yang dapat menanggulangi kejahatan terhadap teknologi informasi.

Peraturan terhadap teknologi informasi agar diterima masyarakat harus mempertimbangkan semua aspirasi (suprastruktur, infrastruktur, kepakaran dan aspirasi internasional) dan berbagai kepentingan harus diselaraskan dan diserasikan. Persoalan komunikasi massa menempati posisi yang strategis dalam kehidupan demokrasi, dan ini akan bersentuhan secara langsung tidak hanya dengan persoalan supremasi hukum yang bersifat *"top down"* misalnya untuk kepentingan keamanan Negara, persatuan dan kesatuan nasional tetapi juga sebaliknya, "*bottom up*", sebab orang cenderung akan melemparkan banyak pertanyaan kritis.[26]

b. Kebijakan Formulasi dalam Undang-Undang No.11 Tahun 2008 tentang informasi dan Transaksi Elektronik

[26] Muladi, Demokrasi, *Hak Asasi Manusia dan Reformasi Hukum di Indonesia*, Habibie Center, Jakarta, 2002, hlm.201.

Negara Indonesia telah membuat kebijakan yang berhubungan dengan hukum teknologi informasi (*law of information technology*) setelah diundangkannya Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada tanggal 21 April 2008 oleh Menteri Hukum dan Hak Asasi Manusia. Produk hukum yang berkaitan dengan ruang siber (*cyber space*) atau mayantara ini dianggap oleh pemerintah perlu untuk memberikan keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal.

Kritik masyarakat baik dari akademisi, aparat penegak hukum, para *bloggers* terutama *hackers* pada saat disahkannya UU ITE adalah hal yang wajar di era demokratisasi seperti saat ini. Karena dalam merumuskan peraturan hukum dewasa ini harus mempertimbangkan secara komprehensif beragam dimensi persoalan. Di sini orang akan mempersoalkan hak-hak warga seperti kebebasan berekspresi, kebebasan media, dan masalah-masalah HAM seperti : persoalan privasi, hak untuk memperoleh informasi, dan sebagainya yang saat ini sangat diperhatikan dalam legislasi positif nasional. Di sinilah relevansi persoalan hak dan kewajiban menjadi penting.

Penanggulangan kejahatan di dunia maya tidak terlepas dari kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah "politik criminal" menurut Sudarto politik criminal merupakan suatu usaha yang rasional dari masyarakat dalam menanggulangi kejahatan.[27]

Evaluasi terhadap kebijakan di dunia mayantara tetap diperlukan sekiranya ada kelemahan kebijakan formulasi dalam perundang-undangan tersebut. Menurut Barda Nawawi Arief Evaluasi atau kajian ulang ini perlu dilakukan, karena ada keterkaitan erat antara kebijakan formulasi perundang-undangan (*legislative policy*)

[27] Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 2007, hlm.38.

dengan kebijakan penegakan hukum (*law enforcement policy*) dan kebijakan pemberantasan/penanggulangan kejahatan (*criminal policy*). Kelemahan kebijakan formulasi hukum pidana, akan berpengaruh pada kebijakan penegak hukum pidana dan kebijakan penanggulangan kejahatan.[28]

Dilihat dari perspektif hukum pidana maka kebijakan formulasi harus memperhatikan harmonisasi internal dengan sistem hukum pidana atau aturan pemidaan umum yang berlaku saat ini. Tidaklah dapat dikatakan terjadi harmonisasi apabila kebijakan formulasi berada diluar sistem hukum pidana yang berlaku saat ini.

Kesimpulan

Pada saat ini eksistensi dari Denial of Service (DoS) Attack telah menjadi suatu masalah yang serius, Karena DoS Attack ini berpotensi untuk menghancurkan perekonomian suatu Negara, dikarenakan dari fungsi DoS Attack ini yang mana mampu menghancurkan sistem perbankan sehingga data nasabah bank yang di serang tersebut menjadi tidak valid lagi (rusak). Karena berdasarkan pengertiannya DoS Attack ialah serangan yang membuat server tidak bisa melayani pengguna yang sesungguhnya, DoS Attack melanggar Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik pasal Pasal 31 ayat (2), Pasal 32 ayat (1), Pasal 33, dan Pasal 36. Pelaku tindak pidana mayantara DoS Attack dapat menerima sanksi yang berat baik kurungan ataupun denda yang besar.

Saran

Diharapkan agar pelaku DoS Attack yang telah merugikan banyak pihak dapat diadili sesui dengan ketentuan UU No.11 Tahun 2008 tentang ITE, yaitu Pasal 31 ayat (2), Pasal 32 ayat (1), Pasal 33, dan Pasal 36. Untuk mengurangi pelaku DoS Attack

[28] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Prenada Media Group, Jakarta, 2008, hlm.214-215.

sebaiknya masyarat harus diberi pembelajaran tentang moral secara lebih baik dan pemerintah juga ikut andil dalam menggalakkan hal tersebut. Agar orang yang mendalami ilmu tentang komputer tidak melakukan DoS Attack, apalagi DoS Attack yang dilakukan merugikan banyak pihak, seperti DoS Attack terhadap sistem perbankan.

Daftar Pustaka

A. Referensi Buku

Barda Nawawi Arief, *Antisipasi Penanggulangan* "*Cybercrime*" *dengan hukum Pidana*, PT RajaGrafindo, Jakarta

Efzy Zam, *Buku Sakti Hacker*, Mediakita, Jakarta, 2011

Lili Rasjidi, *Dasar-Dasar Filsafat dan Teori Hukum*, Citra Aditya Bakti, Bandung, 2001Moeljatno, *Azas-Azas Hukum Pidana*, Bandung: Bina Aksara, 1987

Muladi, *Demokrasi, Hak Asasi Manusia dan Reformasi Hukum di Indonesia*, Habibie Center, Jakarta, 2002,

O.C.Kaligis, *Penerapan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Prakteknya*, Yarsif Watampone, Jakarta, 2012

Onno W Purbo, *Kebangkitan Nasional Ke-2 Berbasis Teknologi Informasi, Computer Network Research Group*, ITB, 2007

B. Perundang-undangan

Undang-undang Dasar Negara Republik Indonesia Tahun 1945 (amandemen).

Kitab Undang-undang Hukum Pidana

Kitab Undang-undang Hukum Acara Pidana

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektroni (UU ITE)

Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

C. Sumber Lain

www.tempo.com

www.wordpress.com

www.blogspot.com

www.yahoo.com

www.google.com