Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

TINDAK PIDANA DUNIA MAYA BERUPA VIRUS DAN TROJAN HORSE MENURUT UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Marco Orias*
marcoori2703@gmail.com

ABSTRACT

Cybercrime or crime at cyberspace has many forms or shapes, but from that all existing's forms, hacking is a forms that gets a lot of attention at the UN Congress X in Vienna st hacking is The first crime, also seen from The technical aspects, hacking have excess. First, The man who hacking must be can do other forms of cybercrime with ability to enter into computer system and then broke that system. Second, technically the quality of the hacking result from hacking that more seriously if compared with other forms of cybercrime, such as viruses and The Trojan Horse. Computer media and cyber world becomes most targets that attack by hackers because regarded as media that common owned by all levels of society. As that becomes problem in this research is how an arrangement crime of Virus and The Trojan Horse, and how the law enforcements tackling crime of Virus and The Trojan Horse. Research approach used normative juridical, the collected data both primary and secondary data examine by juridical review with not eliminate other nonjuridical element. This approach leads to laws and regulations as a major study of law and behavior of the perpetrator that wrongly use technology and information as concrete support to strengthening that juridical analysis. Result of research indicated that the role of law enforcement in handling crimes of Viruses and Trojan Horse that exercised so far was still very minimal.This cause many obstacles found by law enforcements, the existing statuary barriers, constraints of investigation, and the resistance of the people themselves.The most important thing is the system verification in order to cope with the crime of Viruses and Trojan Horse through repair or revision of existing statuary barriers, whether Law No.11 Year 2008 and The other regulation that related with The crimes of Viruses and The Trojan Horse.

Keyword : Criminal Act, Cyberspace, Viruses, and The Trojan Horse

ABSTRAK

Kejahatan dunia maya atau kejahatan di dunia maya memiliki banyak bentuk, tetapi dari itu semua bentuk yang ada, peretasan adalah bentuk yang mendapat banyak perhatian di Kongress PBB X di Wina, mengatur peretasan adalah kejahatan pertama, juga dilihat dari aspek teknis, peretasan memiliki kelebihan , pertama orang yang melakukan peretasan harus bisa melakukan bentuk lain cybercrime dengan kemampuan masuk ke sistem computer dan kemudian merusak sistem itu. Kedua, secara teknis kualitas hasil peretasan dari peretasan itu lebih serius jika dibandingkan dengan bentuk-bentuk cybercrime lainnya, seperti Virus dan Trojan Horse. Media computer dan dunia cyber menjadi sasaran terbanyak yang diserang oleh para peretas karena dianggap sebagai media yang umum dimiliki oleh semua lapisan masyarakat. Adapun yang menjadi masalah dalam penelitian ini adalah bagaimana suatu pengaturan kejahatan Virus dan Trojan Horse dan bagaimana penegakan hukum yang menangani kejahatan Virus dan Trojan Horse. Pendekatan penelitian menggunakan yuridis normatif, data yang dikumpulkan baik data primer maupun sekunder ditelaah oleh kajian yuridis dengan tidak menghilangkan unsur non yuridis lainnya. Pendekatan ini mengarah pada hukum dan perilaku pelaku yang salah menggunakan teknologi dan informasi sebagai dukungan kongkrit untuk memperkuat analisis yuridis tersebut. Hasil penelitian

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

menunjukkan bahwa peran penegak hukum dalam menangani kejahatan Virus dan Trojan Horse yang dilakukan selama ini masih sangat minim. Hal ini menyebabkan banyak hambatan yang ditemukan oleh penegak hukum, hambatan hukum yang ada, kendala penyelidikan , dan perlawanan masyarakat itu sendiri. Yang paling penting adalah verifikasi sistem untuk mengatasi kejahatan Virus dan Trojan Horse melalui perbaikan atau revisi baru hukum yang ada, apakah UU No.11 Tahun 2008 dan Peraturan lain yang terkait dengan Kejahatan Virus dan Trojan Horse.
Kata Kunci : Tindakan kriminal, Cyberspace, Virus, dan Trojan Horse.

1. PENDAHULUAN

Teknologi Informasi (selanjutnya disebut TI) berkembang dengan pesat menyebabkan banyak perubahan pada segi kehidupan sosial masyarakat baik ekonomi bisnis, sosial politik, sistem komunikasi dan interaksi, pendidikan, termasuk juga hukum.TI internet pada awalnya dikembangkan semata-mata untuk memudahkan manusia dalam menjalankan rutinitas kehidupannya. Internet, sesungguhnya merupakan suatu jaringan besar yang terdiri dari jumlah besar jaringan komputer dari seluruh dunia saling terhubung antara satu dengan yang lainnya. Masyarakat penggunanya kemudian dikenal dengan istilah global community dan mereka seakan-akan mendapati satu dunia baru yang dinamakan dunia maya (cyber space).

Cyber Crime dapat diartikan sebagai perbuatan melawan hukum dan/atau tanpa hak berbasis TI atau dengan memakai komputer dan/atau jaringan komputer sebagai sarana atau alat sehingga menjadikan komputer dan/atau jaringannya sebagai obyek maupun subyek tindak pidana yang dilakukan dengan sengaja. Selanjutnya dalam catatan ini saya memakai cyber crime sebagai tindak pidana TI dalam kaitannya dengan tindak pidana yang tidak diatur secara khusus dalam Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP). Kejahatan yang seringkali berhubungan dengan internet antara lain penyebaran Virus dan *Trojan Horse* sebagai kejahatan yang dapat dilakukan melalui kecanggihan TI dan komunikasi dalam hal ini melalui penyalahgunaan media internet. *The Trojan Horse*, diartikan sebagai suatu prosedur untuk menambah, mengurangi atau mengubah instruksi pada sebuah program, sehingga program tersebut selain menjalankan tugas yang sebenarnya juga akan melaksanakan tugas lain yang tidak sah. Tindakan ini dapat dikategorikan sebagai tindak pidana penggelapan (Pasal 372 dan 374 KUHP). Ketika berhadapan dengan tindak pidana penyebaran Virus dan *Trojan Horse* menimbulkan masalah baru yang akan muncul, karena dalam hukum acara pidana yang berlaku tidak diatur mengenai alat bukti elektronik. Namun demikian, saat ini telah berlaku UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK (selanjutnya disebut UU ITE) yang

didalamnya mengatur berbagai aktifitas yang dilakukan dan terjadi di dunia maya, termasuk pelanggaran hukum yang terjadi. Salah satu pelanggaran hukum tersebut adalah penyebaran Virus dan *Trojan Horse*. UU ITE telah mengatur tentang pembuktian yang menyangkut TI termasuk internet, tetapi masih banyak kendala-kendala dalam kenyataannya sehingga seringkali pelaku penyebaran Virus dan *Trojan Horse* melalui internet lolos dari jeratan hukum. UU ITE ini mempunyai 13 (tiga belas) Bab dan 54 (lima puluh empat) Pasal di dalamnya yang mengatur berbagai kegiatan di dunia siber serta menerapkan azas-azas Ekstra Teritorial. Azas Kepastian Hukum, Azas Manfaat, Azas Kehati-hatian, Azas Itikad Baik dan Azas Netral Teknologi.

Pemanfaatan Internet tidak hanya membawa dampak positif, tapi juga dampak negatif. Salah satu dampak negatif dari pemanfaatan internet adalah penyebaran Virus dan *Trojan Horse* yang menjadi perhatian serius Pemerintah di berbagai Negara termasuk Indonesia. Kejahatan ini merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Kekhawatiran demikian terungkap pula dalam makalah "*cyber crime*" yang disampaikan oleh *Information Technology Association of Canada* (ITAC) pada "*International Information Industry Congress (IIC) 2000 MelleniumCongress*" di quebec pada tanggal 19 September 2000, yang menyatakan bahwa "*cyber crime is a real and growing threat to economic and social development around af human life and so can electronically enabled crime*".

Pada dasarnya masyarakat Indonesia harus mendapat perlindungan hukum dari dampak yang diakibatkan oleh berbagai kejahatan yang terjadi baik secara nyata maupun di dunia maya, termasuk tindak pidana penyebaran Virus dan *Trojan Horse* melalui internet. Perlindungan terhadap masyarakat tersebut terkandung dalam Pembukaan Undang-Undang Dasar 1945 alinea keempat yang menyebutkan bahwa :

"Kemudian daripada itu untuk membentuk suatu Pemerintah Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum,…".

Amanat dalam alinea keempat Pembukaan Undang-Undang Dasar 1945 tersebut merupakan konsekuensi hukum yang mengharuskan pemerintah tidak hanya melaksanakan tugas pemerintahan saja, melainkan juga kesejahteraan sosial melalui pembangunan nasional. Selain itu juga merupakan landasan perlindungan hukum kepada masyarakat, karena kata "melindungi" mengandung asas

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

perlindungan hukum bagi segenap bangsa Indonesia untuk mencapai keadilan. Pada dasarnya, Indonesia telah berusaha mengantisipasi adanya dampak dari tindak pidana dunia maya terhadap masyarakat, melalui beberapa tindakan baik secara preventif, antisipatif maupun secara represif.

Proses penegakan hukum di Indonesia sampai saat ini masih terus dilakukan. Kerjasama antara sesama penegak hukum (Polisi, Jaksa, Hakim dan Advokat) terus dijalin dalam mengatasi semua permasalahan hukum baik di bidang perdata, pidana, tata usaha negara dan lingkup peradilan lainnya. Sampai saat ini, tingkat kejahatan di Indonesia terus melaju cepat seiring dengan perkembangan TI dan telekomunikasi yang semakin canggih. Pesatnya TI dan telekomunikasi ini selain memberikan manfaat bagi masyarakat di satu sisi, sering pula disalahgunakan sehingga menimbulkan perbuatan melawan hukum, tidak terkecuali pada tindak pidana penyebaran Virus dan *Trojan Horse* melalui internet.

1. Pengertian Virus dan Trojan Horse

> Virus komputer adalah suatu program komputer yang menduplikasi atau menggandakan diri dengan menyisipkan salinannya ke dalam media penyimpanan dokumen serta ke dalam jaringan komputer secara diam-diam tanpa sepengetahuan pengguna komputer tersebut. Efek dari virus komputer ini sangat beragam mulai dari munculnya pesan-pesan aneh, sampai pada tahap merusak dokumen atau file dan bahkan dapat merusak jaringan komputer itu sendiri. *Trojan Horse* sebagai program yang bekerja lebih dari yang diharapkan, misalnya seorang pemakai menggunakan program pengolah kata, maka program ini dapat dianggap *Trojan* bila tanpa kehendak pemakai tiba-tiba melakukan perintah *format* (hapus) pada *hard disk*. Cukup sulit untuk mendeteksi apakah suatu program berupa *Trojan* atau tidak. Biasanya hal ini diketahui belakangan, terutama karena efek samping yang benar-benar buruk. Istilah *Trojan* sendiri diambil dari suatu kisah pada era Yunani dan kerajaan Troya.

Sedangkan *Trojan Horse* atau Kuda Troya atau yang lebih dikenal sebagai *Trojan* dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigaan (*malicious software/malware*) yang dapat merusak sebuah sistem jaringan.

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

Tujuan dari *Trojan* adalah memperoleh informasi dari target (password, kebiasaan *user* yang tercatat dalam *systemlog*, data dan lain-lain).

Beberapa jenis *Trojan* yang beredar antara lain adalah :

1. Pencuri *password* : Jenis *Trojan* ini dapat mencari password yang disimpan di dalam sistem operasi (/etc/password atau /etc/shadow dalam keluarga sistem operasi UNIX atau berkas *Security Account Manager* (SAM) dalam keluarga sistem operasi *Windows NT* dan akan mengirimkannya kepada si penyerang yang asli. Selain itu, jenis *Trojan* ini juga dapat menipu pengguna dengan membuat tampilan seolah-olah dirinya adalah layar *login* (/sbin/login dalam system operasi UNIX atau *Winlogon.exe* dalam sistem operasi *Windows NT*) serta menunggu pengguna untuk memasukkan passwordnya dan mengirimkannya kepada penyerang. Contoh dari jenis ini adalah *Passfilt.dll* yang aslinya digunakan untuk menambah keamanan *password* dalam sistem operasi Windows NT, tapi disalahgunakan menjadi sebuah program pencuri *password.*

2. Pencatatan penekanan tombol (*keystroke logger/keylogger*) : Jenis *Trojan* ini akan memantau semua yang diketikkan oleh pengguna dan akan mengirimkannya kepada penyerang. Jenis ini berbeda dengan *spyware,* meski dua hal tersebut melakukan hal yang serupa (memata-matai pengguna).

3. Tool administrasi jarak jauh (Remote Administration Tools/RAT) : Jenis *Trojan* ini mengizinkan para penyerang untuk mengambil alih control secara penuh terhadap sistem dan melakukan apapun yang mereka mau dari jarak jauh, seperti mem*format hard dis*k, mencuri atau menghapus data dan lain-lain. Contoh dari Trojan ini adalah *Back Orifice, Back Orifice 2000*, dan *SubSeven.*

4. *Dos Trojan* atau *Zombie Trojan*: Jenis *Trojan* ini digunakan untuk menjadikan sistem yang terinfeksi agar dapat melakukan serangan penolakan layanan secara terdistribusi terhadap *hosttarget.*

5. Ada sebuah jenis *Trojan* yang menggabungkan dirinya sendiri ke sebuah program untuk memodifikasi cara kerja program yang disusupinya. Jenis *Trojan* tersebut sebagai *Trojan* virus.

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

6. *Cookies Stuffing*, ini adalah script yang termasuk dalam metode *blackhat*, gunanya untuk membajak *tracking code* penjualan suatu produk, sehingga komisi penjualan diterima oleh pemasang *cookies stuffing*, bukan oleh orang yang terlebih dahulu merefensikan penjualan produk tersebut di internet.

Berikut 5 jenis *Trojan Hors*e yang teknik serangannya dengan cara mengelabui sistem pengamanan :

1.*Glieder Trojan*

Trojan ini seolah mengatakan "jangan hiraukan saya, saya disini hanya untuk mengistirahatkan computer ini."Padahal sesungguhnya computer sedang memasukkan sebuah program pengintai.

Glieder Trojan menggunakan proses penularan bertingkat, dimana tahap pertamanya adalah sebuah malware kecil akan berubah secara terus-menerus, sehingga program anti-virus yang terpasang dalam PC tidak akan mengenalnya sebagai malware.

Begitu *Glieder Trojan* terinstal dalam PC, program ini akan berusaha menghilangkan kemampuan sistem pengamanan yang terpasang, baru setelah itu melakukan aktifitas jahatnya seperti memindahkan atau mencuri data penting, atau aktifitas lainnya sesuai keinginan penyerang.

2. *Gozi Trojan*

Websites dapat menggunakan *secure cocket layer* (SSL) untuk menyandi dan mengamankan data penting dan sensitive seperti on-line banking atau transaksi on-line. Ciri-ciri yang menggunakan SSL adalah adanya gambar gembok di *address bar*-nya.

Gozi Trojan seolah mengatakan "website dikunci dan disandi? no, problem !" dan dia akan menghindari pengamanan ini (SSL) dengan cara mengelabuhi OS Windows, sehingga seakan-akan dia adalah bagian dari proses SSL.

Yang terjadi adalah data meninggalkan browser melalui *Gozi Trojan* sebelum data tersebut disandikan dan dikirimkan keluar PC menuju network. Program jahat ini memang tidak seperti

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

Trojan pada umumnya, dia masuk sampai ke operating sistem dengan mengelabuhi *layered service providers* (LSPs).

3. *SpamThru Trojan*

Program jahat ini berlaku seolah-olah sebuah program anti-virus tambahan, sehingga dapat dikatakan "*malware* yang melakukan scanning *malware* dalam PC". Bila PC memasang anti-virus baru yang lebih baik, dia akan memblok *malware* ini agar tidak bisa melakukan up-date yang dapat mengubah dirinya menjadi *malware* lain.

4. *SpyAgent Trojan*

Program ini bermain di area penyandian file dalam windows, yaitu ketika kita melakukan penyandian dengan fasilitas yang disediakan oleh windows. *Spy Agent* ini memposisikan dirinya sebagai user account tingkat administrator, dan menggunakan account tersebut untuk menyandi file-file, program anti-virus yang terpasang tidak akan menduga adanya file yang sudah disusupi program jahat.

5. *Jowspry Trojan*

Jowspry Trojan mengelabuhi PC dengan teknik topeng (*masquerader*), seolah-olah sebuah program yang memang sudah dikenal dan diakui oleh PC, yaitu *windows up-date*.

Program ini akan melakukan koneksi seperti background intelligent transfer service yang digunakan oleh program windows up-date, sehingga tidak ditangkal oleh program *firewall* yang terpasang dalam PC. Seolah mengatakan "hai *firewall*, saya *windows up-date*, jangan khawatir la yaw!".

Penyebaran virus dan *Trojan Horse* bisa melalui banyak cara, diantaranya yang paling sering, antara lain:

1. Menggunakan disket yang sebelumnya sudah tertular virus (dari orang lain/komputer lain). Penularan bisa terjadi baik pada saat membaca file, meng*copy file* atau bahkan hanya perintah *dir* (melihat daftar isinya saja).

2. Software bajakan, ada beberapa software bajakan yang beredar di Indonesia (dalam bentuk CD) yang berisikan virus. Diantaranya Windows 98, Dr.Hacker and Mrs.Crack, Power Utilities volume 2,

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

juga beberapa CD games. Termasuk juga file MP3 yang cukup terkenal itu, beberapa diantaranya mengandung virus baik secara disengaja maupun secara tidak sengaja terinfeksi virus.

3. Melalui Internet, terutama jika anda menerima *email* yang ada *attachement*-nya dari orang yang tidak dikenal (ataupun yang dikenal sekalipun). *Email* yang perlu dicurigai mengandung virus, jika ada *attachment*/lampiran file: *.zip, *.com, *.exe, *.doc, *.rtf, *.dll, *.xls, *.pps, *.ppt, sebaiknya diperiksa terlebih dahulu dengan antivirus. Apalagi jika anda menerima *email* dengan *attachement* bernama Zipped_files.exe sebaiknya segera hapus file tersebut (virus worm *explorer*). Sedang *email* tanpa *attachement* dipastikan bebas virus.

4. Melalui Internet, saat mengunjungi / mendownload sesuatu di situs (alamat) tertentu, misal situs *hacker*, situs porno, ataupun situs lainnya yang tidak jelas pengelolanya patut dicurigai. Apalagi dengan adanya virus baru yang dibuat dengan bahasa pemrogaman *java*, pada saat mengunjungi site tersebut virus *java* dapat langsung menulari komputer tanpa disadari.

PEMBAHASAN

1. Kasus-kasus Terkait Dengan Penyebaran Virus dan *Trojan Horse*

Beberapa saat lalu di dunia dihebohkan dengan virus Chernobyl (CIH), yang dapat merusak data di hard disk dan juga menghapus BIOS (untuk motherboard yang memakai flashbios yang tidak diproteksi). Sehingga mengakibatkan kerugian cukup besar. Saat ini ada ancaman serupa dengan virus CIH (Chernobyl), yang telah dapat dideteksi kehadirannya. Virus ini akan menyerang pada tanggal 25 Desember tiap tahunnya.

1. Virus tanggal 25 Desember yaitu Win32.Kriz, Win32Kriz.3270, Win32Kriz.3862, dan masih akan bertambah variannya (jenisnya). Type:Polymorphic virus (dapat menyembunyikan identitasnya setiap kali menginfeksi), saat aktif tanggal 25 Desember tiap tahun. Aksinya mirip virus Chernobyl tetepi lebih ganas (merusak data di hard disk, merusak CMOS dan BIOS), dan juga memberikan message / pesan anti agama.
2. Virus Prilissa, merupakan varian virus Melissa variant (Prilisia), yang pada hari natal dapat memformat hard disk. Prilissa menginfeksi dokumen Word 97 dan menyebar lewat attachment email. Saat dokumen yang terinfeksi dibuka, virus mematikan setting sekuriti proteksi virus, konfirmasi konversi dan membuka file list. Prilissa diekskusi di sistem, kemudian menduplikat

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

dirinya dengan mengirim email menggunakan MS Outlook ke 50, email address pertama yang terdapat di address list. Message berisi Message From (username) yang mana user namenya adalah user name system. Body message nya berisikan kalimat 'This document is very Importantand you've GOT to read this'.

Virus *Melissa Love Letter* muncul di Amerika Serikat, variannya *very Funny Joke* langsung muncul dalam beberapa saat, diikuti dengan lebih dari 30 jenis lainnya dalam dua bulan kemudian.

Ada beberapa kasus penyebaran virus komputer lainnya di tahun 2003, yaitu :

1. *Randon* menyebarkan dirinya melalui IRC chat channels dan komputer yang disharing terhubung di dalam sebuah jaringan. Yang paling adalah mempunyai ciri-ciri yang khusus yaitu mempunyai *malicious code* yang merupakan sebuah dropper jenis worm yang menyusup pada beberapa file di komputer yang terinfeksi, beberapa diantaranya adalah virus yang mempunyai efek yang dapat berubah-rubah. *Actions They carry out include opening ports, running applications, propagating* dan memasukkan *Denial of Service* (DoS) serta membanjiri dengan penyerangan, dan lain-lainnya. Randon dapat menghubungi ke *web page* dan mendownload sebuah backdoor jenis *Trojan*. Sebuah petunjuk kehadiran dari worm ini di dalam sebuah komputer adalah adanya peningkatan *network traffic* melalui *ports* 445 dan 6667.
2. *Worm Lentin.P* menyebar melalui *email* dalam sebuah message dengan ciri khas yang berubah-rubah.

Pada Maret 2003, empat buah virus yang cukup berbahaya telah ditemukan. Virus tersebut antara lain *NiceHello, CodeRed.F, Deloder.A* dan *Prom* serta sebuah Virus *Trojan* yang dikenal sebagai SysComm. *Worm* yang kedua adalah *CodeRed.F*, ini adalah varian dari virus *worm* yang dikenal sebagai *CodeRed.IIS.2*, dimana perbedaannya hanya 2 byte saja dari virus *CodeRed* yang aslinya. Modifikasi ini memungkinkan *CodeRed.F* terus-menerus menyebar sampai tahun 34952, mengingat virus *worm CodeRed.IIS.2* hanya berfungsi sampai akhir tahun 2002. *CodeRed.F* memanfaatkan kelemahan pada Index Server 2.0, Indexing Service dan Internet Information Server (versions 4.0 dan 5.0). Virus *worm* yang ketiga adalah *Deloder.A*, yang menyebar melalui networking dan internet, serta dapat mematikan *sharing resource : CS, DS, ES, ADMINS dan IPCS*. *Worm Prom*, hanya menginfeksi komputer yang dijalankan dengan menggunakan system operasi Windows XP/2000/NT. Virus ini menyebar melalui *email* dalam sebuah *message* yang sulit dikenal, karena ia mempunyai karakter yang berubah-rubah. Akhirnya, jenis virus kali ini ditutup dengan

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

varian dari virus worm *Lovgate 'F' dan 'G'*, yang mana virus-virus tersebut menyebar melalui email dan networking. Kasus serangan terhadap *13root server DNS* adalah salah satu contoh peran *Trojan Horse* dalam serangan internet. Komputer-komputer zombie yang disinyalir FBI berada di AS dan Korsel itu adalah komputer-komputer korban Kuda Troya. Dengan masuknya *Trojan Horse* kedalam sistem tersebut, sistem-sistem itu diambil alih kendalinya oleh penyerang sesungguhnya (master). Serangan DDOS yang sempat melumpuhkan situs raksasa *Yahoo.com* dan *Amazon.com* juga dilakukan dengan memanfaatkan *Trojan Horse*. Ancaman lain *Trojan Horse* dalam dunia *cyber* adalah pencurian informasi pribadi seperti nomor PIN Internet banking, pencurian password email, dan pencurian kartu kredit.

Pencurian informasi pribadi semacam itu sangat mudah dilakukan jika komputer korban telah disusupi *Trojan Horse*. Karenanya sangat disarankan untuk tidak sembarangan menjalankan program-program yang tidak dikenal dan juga tidak menggunakan komputer publik, misalnya komputer warnet, untuk melakukan transaksi yang penting.

Dengan masuknya *Trojan* tertentu ke dalam sebuah komputer, aktifitas yang ada pada komputer korban tersebut dapat dimonitor oleh penyerang yang menyusupkan *Trojan Horse*. Aktifitas korban juga setiap saat dapat dimonitor oleh penyerangnya.

Mencermati berbagai ciri kejahatan dunia maya, dapat saja kita berspekulasi akan terbentuk suatu golongan elit pelaku kejahatan *cyber*. *Cyberlaw* sebagai antisipasi hukum terhadap hal ini sangat diperlukan, karena intelektualitas dan penguasaan teknologi tinggi terlibat di dalamnya. Ada dua pilihan terhadap kebijakan hukum pidana terhadap *cybercrime* khususnya penanggulangan terhadap kejahatan *hacking*.

Pertama, aturan ini cukup dimasukkan dalam konsep rumusan KUHP baru, sehingga aturan ini bersifat umum (*lex generalis*). Kedua, perlu diatur dalam undang-undang yang bersifat khusus (*lex specialis*). Kalangan pakar keamanan data Amerika Serikat menyebut kejahatan *cyber* sebagai "*unsmoking gun*", karena kejahatan tersebut tidak memberikan suatu indikasi apapun yang memperingatkan terjadinya kesalahan. Kejahatan *cyber* dalam komunitas global masyarakat pengguna internet adalah suatu hal yang dapat disadari atau tanpa disadari, sengaja atau tidak sengaja dilakukan. Hal ini terjadi karena perkembangan teknologi informasi dan tingkat intelektualitas/intelegensia masyarakat yang semakin meningkat. Faktor internet itu sendiri juga

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

menimbulkan selentingan-selentingan maya pada pengguna internet untuk terus dan terus mencari dan mencoba.

Modus Tindak Pidana *Cybercrime* antara lain Pertama, kejahatan yang memanfaatkan jaringan informasi dan tampilan data yang ada didalam internet untuk mempengaruhi pengambilan keputusan sebuah investasi yang berlangsung secara *online* dengan secara otomatis hal itu akan berdampak terhadap pergerakan harga saham-saham dilantai bursa. Penipuan informasi internet inilah yang merupakan landasan pertama yang paling sering memenuhi unsur atas penipuan dari sebuah penawaran sahan yang tidak memiliki fakta material sesungguhnya; Kedua, kejahatan internet yang bersumber pada sebuah tujuan untuk mencuri atau menghancurkan sebuah produk ataupun informasi yang bersifat sebagai asset dari sebuah jaringan internet lainnya dimana pencurian ini dapat menimbulkan kerugian atau menciptakan sebuah kekuatan untuk menghancurkan atau mengambil alih sasaran ekonomis yang telah ditargetkan secara *online*; Ketiga, kejahatan internet yang bersifat kerahasiaan negara ataupun yang bertujuan untuk merusakkan sebuah jaringan dari sistem keamanan sebuah negara.

Berita Kompas *Cyber* Media (19/3/2002) menulis bahwa berdasarkan survey AC Nielsen 2001 Indonesia ternyata menempati posisi ke enam terbesar di dunia atau keempat di Asia dalam tindak kejahatan di internet. Meski tidak disebutkan secara rinci kejahatan macam apa saja yang terjadi di Indonesia maupun WNI yang terlibat dalam kejahatan tersebut, hal ini merupakan peringatan bagi semua pihak untuk mewaspadai kejahatan yang telah, sedang, dan akan muncul dari pengguna TI.

Menurut Rommy Alkatiry (Wakil Kabid Informatika KADIN), penyalahgunaan kartu kredit milik orang lain di internet merupakan kasus *cybercrime* terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau *online*. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi pembelian barang di internet.

Menurut John S. Tumiwa pada umumnya tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia baru sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank.

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

Contoh-contoh kasus setelah tahun 2004 : yang terjadi adalah pencurian dokumen terjadi saat utusan khusus Presiden Susilo Bambang Yudhoyono yang dipimpin Menko Perekonomian Hatta Rajasa berkunjung di Korea Selatan. Berdasar informasi dari Kemhan, data yang diduga dicuri merupakan rencana kerja sama pembuatan 50 unit pesawat tempur di PT. Dirgantara Indonesia (DI). Pihak PT.DI membenarkan sedang ada kerja sama dengan Korsel dalam pembuatan pesawat tempur KFX (*Korea Fighter Experiment*). Pesawat KFX lebih canggih daripada F16.

Jaringan internet di Pusat Tabulasi Nasional Komisi Pemilihan Umum sempat down (terganggu) beberapa kali. KPU menggandeng kepolisian untuk mengatasi hal tersebut. "Cybercrime kepolisian juga sudah membantu. Domain kerjasamanya antara KPU dengan kepolisian", kata Ketua Tim Teknologi Informasi KPU, Husni Fahmi di Kantor KPU, Jalan Imam Bonjol, Menteng Jakarta Pusat (15 April 2009). Menurut Husni, tim kepolisian pun sudah mendatangi Pusat Tabulasi Nasional KPU di Hotel Borobudur, Jakarta Pusat. Mereka akan mengusut adanya dugaan kriminal dalam kasus kejahatan dunia maya dengan cara meretas.

Penggunaan media internet para teroris di Asia Tenggara menunjukkan peningkatan yang signifikan, kelompok yang sering dituding oleh dunia barat sebagai ekstrimis itu menggunakan dunia maya untuk menyebarkan ide radikal. Kita harus memperhatikan dengan serius perkembangan dan pergerakan kelompok radikal online tersebut. Modus dari kegiatan kejahatan ini adalah penyebaran ide radikal.

Penyebaran virus dengan sengaja, ini adalah salah satu jenis kasus *cybercrime* yang terjadi pada bulan Juli 2009, *Twitter* (salah satu jejaring sosial yang sedang naik pamor di masyarakat belakangan ini) kembali menjadi media infeksi modifikasi New Koobface, worm yang mampu membajak akun *Twitter* dan menular melalui postingannya, menjangkiti semua follower.

Kasus-kasus tersebut diatas terjadi sebelum diberlakukannya UU ITE pada tahun 2008, sehingga saat itu kasus-kasus yang di proses hanya menggunakan metode penafsiran dengan pasal-pasal pada KUHP. Dengan kehadiran UU ITE sebagai upaya penerapan cyberlaw di secara perorangan, properti/bisnis, termasuk juga melindungi kepentingan pemerintah. Mengingat peran pemerintah adalah untuk memfasilitasi implementasi undang-undang tersebut, maka perlu dilakukan sosialisasi secara terus-menerus dengan menggunakan berbagai media yang ada dan itu tidak hanya dilakukan oleh Departemen Komunikasi dan Informatika atau instansi di pusat seperti Dephumkam, Kejaksaan atau kepolisian RI saja melainkan dilakukan pula oleh jajaran pemerintah

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

yang ada di daerah-daerah seperti Dinas Perhubungan, Komunikasi dan Informatika atau dinas-dinas terkait.

Disamping itu, pemerintah segera menerbitkan peraturan pelaksanaannya sebagai panduan pengimplementasikan undang-undang tersebut. UU ITE diharapkan dapat lebih mendorong pengembangan penggunaan teknologi secara lebih meluas, serta sekaligus dapat memberikan keamanan serta kepastian hukum. UU ITE juga untuk melindungi masyarakat dari penyalahgunaan internet yang berimplikasi pada keberlangsungan berbangsa dan bernegara. Dengan adanya UU ITE ini menjadi payung hukum aparat kepolisian untuk bertindak tegas dan selektif terhadap penyalahgunaan internet dan bukan dijadikan alat penjegalan politik dan elit tertentu atau mementingkan segolongan orang, UU ITE juga dapat mengantisipasi kemungkinan penyalahgunaan internet yang merugikan, memberikan perlindungan hukum terhadap kegiatan ekonomi misalnya transaksi dagang atau kegiatan ekonomi lainnya lewat transaksi elektronik seperti bisnis lewat internet dapat meminimalisir adanya penyalahgunaan dan penipuan, sehingga UU ITE juga membuka peluang kepada pemerintah untuk mengadakan program pemberdayaan internet.

2. Pengaturan tindak pidana Virus dan Trojan Horse dengan UU ITE

Berdasarkan Pasal 1 ayat (1) UU ITE, yang dimaksud dengan informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data *interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks ,*telecopy*, atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Selain itu, yang dimaksud dengan sistem elektronik menurut Pasal 1 ayat (5) adalah serangkaian perangkat atau prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi elektronik.

Penafsiran dengan metode yang sama terhadap KUHP sebelum ada UU ITE perlu dilakukan tentang pengertian dalam UU ITE sehingga terdapat batasan dan kejelasan makna agar tidak menimbulkan celah hukum (*loopholes*),yaitu :

‘Melakukan tindakan apapun yang berakibat terganggunya sistem elektronik’

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

Pasal 33 UU ITE menyebutkan bahwa, "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya".

Sehubungan dengan hal itu, setiap orang yang melakukan tindakan apapun yang berakibat terganggunya sistem elektronik karena banyak kegiatan-kegiatan di dunia nyata yang secara nyata tidak ada hubungannya dengan *cybercrime* sehingga kalimat dari pasal ini kegiatan penyebaran Virus dapat dikategorikan sebagi suatu tindak kejahatan.

Pada kasus penyebaran Virus dan*Trojan Horse* ini untuk membuktikannya, dapat dipakai semua alat bukti berbentuk informasi dan/atau dokumen elektronik, namun hal tersebut dapat dijadikan alat bukti sebagaimana ditentukan dalam Pasal 5 ayat (1) UU ITE yang berbunyi :

"Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah".

Dan Pasal 5 ayat (2) UU ITE juga menegaskan bahwa :

"Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat 1 merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia".

Dengan demikian, alat bukti yang digunakan hakim untuk menjatuhkan putusan pada perkara pidana, dapat diperluas menjadi 6 (enam) dari 5 (lima) ketentuan alat bukti sebagaimana telah diatur dalam Pasal 184 KUHAP, yaitu bahwa alat bukti yang sah adalah :

1. Keterangan saksi;
2. Keterangan ahli;
3. Surat;
4. Petunjuk;
5. Keterangan terdakwa;
6. Alat bukti menurut Pasal 5 ayat (1) dan ayat (2) UU ITE.

Meskipun ketentuan mengenai alat bukti di atas merupakan ketentuan hukum acara pidana yang bersifat memaksa (*dwingen recht*), artinya semua jenis alat bukti yang telah di atur dalam pasal tersebut tidak dapat ditambah atau dikurangi.

Secara umum terdapat beberapa teori mengenai sistem pembuktian yakni :

1. *Conviction in time Theory*, yaitu sistem pembuktian yang menyatakan bahwa salah tidaknya seorang terdakwa semata-mata ditentukan oleh penilaian keyakinan hakim. Keyakinan hakim ini dapat diperoleh melalui alat-alat bukti yang diajukan Keterangan Ahli dalam persidangan.
2. *Conviction Raisonee Theory*, merupakan sistem pembuktian berdasarkan keyakinan hakim untuk menentukan salah tidaknya terdakwa, namun dalam sistem ini keyakinan hakim dibatasi dan harus didasari dengan alasan-alasan yang jelas dan dapat diterima yang wajib diuraikan dalam putusannya, sesuai yang diuraikan juga oleh Keterangan Ahli dalam persidangan.
3. Teori Pembuktian Menurut Undang-Undang secara Positif, merupakan pembuktian yang berlatar belakang sistem pembuktian berdasarkan keyakinan atau *Conviction in timeTheory*. Pembuktian pada sistem ini didasari dengan alat-alat bukti yang sah yang telah di tetapkan oleh undang-undang disertai keyakinan hakim dalam menentukan salah tidaknya terdakwa.
4. Teori Pembuktian menurut Undang-Undang Secara Negatif (*Negatief Wettelijkestelsel*), merupakan sistem pembuktian yang menggunakan teori perpaduan antara sistem pembuktian undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *Conviction in time Theory*. Rumusan teori ini adalah bahwa salah tidaknya seorang terdakwa ditentukan oleh keyakinan hakim yang didasarkan pada cara dan dengan alat-alat bukti yang sah menurut undang-undang.

Sementara itu, sistem pembuktian yang dianut oleh KUHAP adalah sistem pembuktian menurut undang-undang secara negatif, karena merupakan perpaduan antara sistem pembuktian menurut undang-undang secara positif dengan sistem pembuktian menurut keyakinan atau *Conviction in time Theory*. Hal ini terlihat dari ketentuan Pasal 183 KUHAP yang menegaskan bahwa: “Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya.”

Berbicara mengenai alat bukti petunjuk ,tidak terlepas dari ketentuan Pasal 188 (2) KUHAP yang membatasi kewenangan hakim dalam memperoleh alat bukti petunjuk, yang secara limitatif hanya dapat diperoleh dari :

1. Keterangan saksi;
2. Surat;
3. Keterangan Terdakwa.

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

Berdasarkan hal tersebut diatas, alat bukti petunjuk hanya dapat diambil dari ketiga alat bukti di atas. Pada umumnya,alat bukti petunjuk baru diperlukan apabila alat bukti lainnya belum mencukupi batas minimum pembuktian yang diatur dalam Pasal 183 KUHAP di atas.

Dengan demikian, alat bukti petunjuk merupakan alat bukti yang bergantung pada alat bukti lainnya yakni alat bukti saksi, surat dan keterangan terdakwa. Alat bukti petunjuk memiliki kekuatan pembuktian yang sama dengan alat bukti yang lain, namun hakim tidak terikat atas kebenaran persesuaian yang diwujudkan oleh petunjuk, sehingga hakim bebas untuk menilai dan mempergunakannya dalam upaya pembuktian. Selain itu, petunjuk sebagai alat bukti tidak dapat berdiri sendiri membuktikan kesalahan terdakwa, karena hakim tetap terikat pada batas minimum pembuktian sesuai ketentuan Pasal 183 KUHAP.

Informasi elektronik atau dokumen elektronik sebagai alat bukti, yang merupakan perluasan dari alat bukti surat sebagai bahan untuk dijadikan petunjuk bagi hakim dalam membuktikan suatu perkara termasuk kasus penyebaran Virus dan *Trojan Horse* yang telah diuraikan pada bagian sebelumnya.

Cyber Crime yang merupakan suatu upaya memasuki atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan melawan hukum atau tanpa menyebabkan perubahan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut atau kejahatan yang dengan menggunakan sarana media elektronik internet (merupakan kejahatan dunia maya) atau kejahatan dibidang komputer dengan secara illegal, dan terdapat definisi yang lain yaitu sebagai kejahatan komputer ditujukan kepada sistem atau jaringan komputer, yang mencakup segala bentuk baru kejahatan yang menggunakan bantuan sarana media elektronik internet.

Dengan demikian *Cyber Crime* merupakan suatu tindak kejahatan didunia alam maya, yang dianggap bertentangan atau melawan undang-undang yang berlaku, oleh karena untuk menegakkan hukum serta menjamin kepastian hukum di Indonesia perlu adanya *Cyber Law* yaitu hukum yang mengatasi kejahatan siber (kejahatan dunia maya melalui jaringan internet). TI menyentuh setiap aspek kehidupan modern dan tidak menutup kemungkinan dapat menimbulkan kejahatan dalam dunia maya. Salah satu kejahatan di dunia maya (*cyber crime*) ini adalah penyebaran Virus dan *Trojan Horse*.

Virus yang merupakan suatu program komputer yang menduplikasi atau menggandakan diri dengan menyisipkan salinannya ke dalam media penyimpanan dokumen serta ke dalam jaringan komputer secara diam-diam tanpa sepengetahuan pengguna komputer tersebut, mempunyai efek

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

sangat beragam mulai dari munculnya pesan-pesan aneh, sampai pada tahap merusak dokumen atau *file* dan bahkan dapat merusak jaringan computer itu sendiri. Virus komputer ini berasal dari penciptaan pengguna computer yang dengan sengaja menyebarkan virus tersebut ke seluruh dunia. Virus computer yang dimaksud sangat beragam dengan nama tersendiri dan daya rusak tersendiri pula.

Trojan Horse atau Kuda Troya atau yang lebih dikenal sebagai *Trojan* dalam keamanan computer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (*malicioussoftware/malware*) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari *Trojan Horse* adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam sistem log, dan data), serta mengendalikan target (memperoleh hak akses pada target). *Trojan Horse* berbeda dengan perangkat lunak mencurigakan lainnya seperti virus komputer atau *worm* karena : *Trojan Horse* bersifat "*stealth*" (siluman dan tidak terlihat) dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik, sementara virus komputer atau worm bertindak lebih agresif dengan merusak sistem atau membuat sistem menjadi crash dan *Trojan Horse* dikendalikan dari komputer lain (komputer *attacker*). Penggunaan istilah *Trojan Horse* dimaksudkan untuk menyusupkan kode-kode mencurigakan dan merusak di dalam sebuah program baik-baik dan berguna ; seperti halnya dalam Perang Troya, para prajurit Sparta bersembunyi di dalam Kuda Troya yang ditujukan sebagai pengabdian kepada Raja Poseidon. Kuda Troya tersebut menurut para petinggi Troya dianggap tidak berbahaya, dan diijinkan masuk ke dalam benteng Troya yang tidak dapat ditembus oleh para prajurit Yunani selama kurang lebih 10 perang Troya bergejolak.

Kebanyakan *Trojan Horse* saat ini berupa sebuah berkas yang dapat dieksekusi (*.EXE atau *.COM dalam sistem operasi Windows dan DOS atau program dengan nama yang sering dieksekusi dalam sistem operasi UNIX, seperti ls, cat, dan lain-lain) yang dimasukkan ke dalam sistem yang ditembus oleh seorang *cracker* untuk mencuri data yang penting bagi pengguna (*password*, data kartu kredit, dan lain-lain). *Trojan Horse* juga dapat menginfeksi sistem ketika pengguna mengunduh aplikasi (seringnya berupa game computer) dari sumber yang tidak dapat dipercayai dalam jaringan internet. Aplikasi-aplikasi tersebut dapat memiliki kode *Trojan Horse* yang diintegrasikan di dalam dirinya dan mengijinkan seorang *cracker* untuk mengacak-acak sistem yang bersangkutan.

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

3. Pembobolan Komputer dan/atau Sistem Elektronik

Larangan melakukan perbuatan membobol sistem komputer yang diatur dalam UU ITE terdiri atas :

a. Membobol komputer dan/atau sistem elektronik yang bertujuan untuk mengakses saja tanpa tujuan lain. Larangan perbuatan ini diatur dalam pasal 30 ayat (1) yang berbunyi :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem Elektronik milik orang lain dengan cara apa pun".

b. Membobol komputer dan/atau sistem elektronik yang selain bertujuan untuk mengakses adalah juga memperoleh informasi elektronik dan/atau dokumen elektronik. Larangan perbuatan ini diatur dalam pasal 30 ayat (2) yang berbunyi :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik".

c. Membobol komputer dan/atau sistem elekronik yang bertujuan selain untuk mengakses juga untuk menaklukkan sistem pengamanan dari sistem komputer yang diakses itu. Larangan perbuatan ini diatur dalam pasal 30 ayat (3) yang berbunyi :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau sistem Elektronik dengan cara apa pun dengan melanggar ,menerobos, melampaui,atau menjebol sistem pengaman".

4. Tindak Pidana Komputer terhadap Sistem Elektronik

Larangan terhadap perbuatan ini di atur dalam pasal 33 yang berbunyi : "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berkaitan terganggunya sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya'.

Tindakan untuk menyebarkan virus dan *Trojan Horse* ini dapat diangap sebagai suatu perbuatan yang layak dipidana, karena sepintas terlihat bahwa pelaku penyebaran virus dan *Trojan Horse* melalui pengiriman email ini memiliki niat untuk merusak dokumen bahkan komputernya, sehingga dapat merugikan pihak lain, dengan demikian terdapat unsur pertanggungjawaban pidana di dalamnya. Perbuatan menyebarkan virus dan *Trojan Horse*

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

melalui pengiriman *email* ini tidak diatur secara spesifik dalam KUHP. Saat ini, walaupun di Indonesia telah ada UU ITE, tetapi tindakan penyebaran virus dan *Trojan Horse* melalui pengiriman *email* juga tidak diatur khusus. Namun demikian Pasal 33 dan Pasal 30 ayat (2) UU ITE yang menegaskan beberapa perbuatan yang dilarang dan diancam sanksi pidana, termasuk larangan mengakses komputer dan atau sistem elektronik pihak lain searah melawan hukum, sehingga perbuatan menyebarkan virus dan *Trojan Horse* dapat dianggap sebagai sebuah tindak pidana.

5. Tanggung jawab Pidana Terhadap Pelaku Penyebaran Virus dan *Trojan Horse* Berdasarkan UU ITE.

Ada beberapa hal yang dapat dilakukan terhadap pelaku penyebaran virus dan *Trojan Horse* ini, yakni : pendekatan teknologi, pendekatan budaya-etika dan pendekatan hukum. Untuk mengatasi gangguan keamanan, pendekatan teknologi mutlak untuk dilakukan, karena tanpa suatu pengamanan melalui teknologi tertentu, maka jaringan akan mudah disusupi, diintersepsi atau diakses secara illegal dan tanpa hak. Pada ruang *cyber* pelaku pelanggaran seringkali menjadi sulit untuk dijerat hukum, karena tidak terpenuhinya unsur-unsur suatu ketentuan hukum, dalam hal ini berhubungan dengan masalah pembuktian. Selain itu, seringkali pengadilan di Indonesia tidak memiliki yurisdiksi terhadap pelaku dan perbuatan hukum yang terjadi, mengingat pelanggaran hukum ini bersifat transnasional yang akibat hukumnya memiliki implikasi hukum di Indonesia. Berdasarkan hukum internasional, terdapat tiga macam yurisdiksi yakni: yurisdiksi untuk menetapkan undang-undang (*The Jurisdiction to prescribe*), yurisdiksi untuk penegakan hukum (*The Jurisdiction to enforce*), dan yurisdiksi untuk menuntut (*The Jurisdiction to adjudicate*).

Berbicara mengenai *cyber spamming* sebagai kejahatan transnasional erat kaitannya dengan beberapa yurisdiksi yaitu yurisdiksi untuk menetapkan undang-undang (*The Jurisdiction to Prescribe*), yurisdiksi untuk menghukum (*The Juridicate to Enforce*) dan yurisdiksi untuk menuntut (*The Jurisdiction Adjudicate*). Pada *The Jurisdiction to Adjudicate* terdapat beberapa asas yang dikenal dalam menentukan hukum yang berlaku yaitu:

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

1. *Asas Subjective Territorial* yaitu berlaku hukum yang menekankan berdasarkan bahwa keberlakuan hukum ditentukan berdasarkan tempat pembuatan dan penyelesaian tindak pidana di lakukan di Negara lain;
2. *Asas Objective Territorial* yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi Negara yang bersangkutan;
3. *Asas Aktif Nationality* yang menentukan bahwa Negara memiliki yurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku;
4. *Asas Passive Nationality* adalah hukum berlaku berdasarkan kewarganegaraan korban;
5. *Asas Protective Principle* adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan di luar wilayahya, dalam hal ini digunakan apabila korban adalah Negara atau pemerintahan;
6. *Asas Protective Principle* adalah berlakunya berdasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan di luar wilayahnya, dalam hal ini digunakan apabila korban adalah Negara atau pemerintahan;
7. *Asas Universality* yang pada mulanya menentukan bahwa setiap Negara berhak untuk menangkap dan menghukum para pelaku (*cybercrime*) kemudian diperluas sampai pada kejahatan terhadap kemanusiaan, dan berlaku untuk lintas Negara terhadap kejahatan yang diangggap sangat serius seperti pembajakan dan terorisme (*crime against humanity*).

Tindak pidana penyebaran Virus dan *Trojan Horse* dimungkinkan melibatkan lebih dari satu sistem atau menyangkut sistem hukum beberapa negara, sehingga dapat dikategorikan sebagai kejahatan transnasional. Pada praktiknya terdapat banyak faktor yang menyebabkan adanya kepentingan lebih dari satu negara dalam suatu kejahatan, baik pelakunya, korbannya, tempat terjadinya kejahatan atau perpaduan unsur-unsur tersebut.

Tindak pidana penyebaran Virus dan *Trojan Horse* dapat melibatkan orang-orang dari berbagai negara, menjadikan sebagai kejahatan transnasional, sehingga dalam proses penegakan hukumnya, harus pula memperhatikan jalinan kerjasama antara kepolisian Indonesia dengan negara-negara lain. Berbicara mengenai *cyber spamming* sebagai kejahatan transnasional erat kaitannya dengan beberapa yurisdiksi yaitu, yurisdiksi untuk menetapkan undang-undang (*TheJuridiction to Prescribe*), yurisdiksi untuk menghukum (*The Juridicate to Enforce*) dan yurisdiksi untuk menuntut (*The Jurisdiction to Adjudicate*). Dengan demikian, tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran Virus dan *Trojan Horse* harus dilakukan sesuai yurisdiksinya dengan memperhatikan hokum yang berlaku.

Apabila telah terbukti bahwa penyebaran Virus melalui pengiriman *email* termasuk perbuatan yang dilarang sebagaimana diatur dalam Pasal 33 UU ITE, maka pelaku dapat dijerat dengan ketentuan ancaman pidana pada Pasal 49 UU ITE yang berbunyi :

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

"Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah)."

Apabila telah terbukti bahwa penyebaran *Trojan Horse* melalui pengiriman *email* termasuk perbuatan yang dilarang sebagaimana diatur dalam Pasal 30 ayat (2) UU ITE, maka pelaku dapat dijerat dengan ketentuan ancaman pidana pada Pasal 46 ayat (2) UU ITE yang berbunyi: "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah)."

Ketentuan tersebut sudah sesuai dengan tindak pidana penyebaran Virus dan *Trojan Horse*, mengingat cakupan wilayah penyebarannya yang transnasional serta dampak kerugian yang ditimbulkan Virus secara umum yakni dapat menyebabkan antara lain: loading start sistem operasi Windows (*98, XP, Vista, Seven*, dll) menjadi lambat, terdapat file yang tidak dapat dibuka (muncul pesan error), bahkan ada file yang hilang meski telah disimpan di *Hard disk* dan media penyimpanan lain seperti Disket, *Flashdisk, Hard Disk External*, dll. Sedangkan dampak kerugian yang ditimbulkan *Trojan Horse* secara umum yakni dapat menyebabkan antara lain: penyusupan pada data *log history* user computer dan pengintaian terhadap data/dokumen dengan *extension**.doc, *.xlx, *.txt; dimana pada umumnya user menyimpan data *user name* maupun *password* untuk akses *e-banking*, dan akses sebagai member dari sebuah toko online atau website jual beli (www.jual beli.com, www.berniaga.com, www.kaskus.co.id, dll), computer beroperasi dengan lambat, terkadang ada file yang tidak dapat dibuka bahkan hilang dari computer dan media penyimpanan data lainnya. Di Indonesia sendiri saya memperkirakan setidaknya ada 1 (satu) dari 3 (tiga) komputer/laptop pasti telah terinfeksi virus / *Trojan Horse* (terutama computer / laptop yang program anti virusnya tidak rutin *update virus definition* secara otomatis dan periodik), sehingga saya menilai bahwa ancaman pidana tersebut diatas cukup berat bagi pelakunya. Sehingga menurut saya tidak perlu ada hukuman minimal dari ancaman pidana penjara dan/atau denda pada Pasal 49 dan Pasal 46 ayat (2) UU ITE, karena dapat dinilai bahwa ancaman pidana tersebut diatas cukup setimpal bagi pelakunya.

PENUTUP

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

Berdasarkan analisis yang telah diuraikan pada bagian sebelumnya, maka dapat disimpulkan hal-hal sebagai berikut :

a. Perbuatan penyebaran Virus dan Trojan Horse melalui email merupakan salah satu perbuatan yang dilarang sebagaimana diatur dalam UU ITE, karena dalam hal ini email dianggap sebagai informasi dan/atau dokumen elektronik yang dapat dijadikan salah satu alat bukti sebagaimana diatur dalam pasal 5 ayat (1) dan (2) UU ITE. Selain itu, email dapat pula dianggap sebagai alat bukti surat yang selanjutnya dijadikan alat bukti petunjuk sesuai ketentuan Pasal 184 KUHAP. Dengan demikian, tindakan penyebaran Virus dapat dijerat dengan Pasal 33 juncto Pasal 49 UU ITE, sedangkan tindakan penyebaran *Trojan Horse* dijerat dengan Pasal 30 ayat (2) juncto Pasal 46 ayat (2) UU ITE.

b. Tindakan hukum yang dapat dilakukan terhadap pelaku penyebaran Virus dan *Trojan Horse* antara lain dengan tuntutan secara hukum dengan memperhatikan yurisdiksi dan hukum yang berlaku, karena hal ini dimungkinkan pelaku berada di negara yang berbeda dengan negara tempat korban kejahatan ini berada, selain itu, sulit pula menentukan tempat kejadian (*locus delicti*) karena kejahatan ini terjadi di dunia maya. Namun demikian yurisdiksi dan hukum yang berlaku dapat ditentukan berdasarkan beberapa asas yang berlaku antara lain Asas *Subjective Territorial* yaitu berlaku hukum berdasarkan tempat pembuatan dan penyelesaian tindak pidana dilakukan di Negara lain, Asas *Objective Territorial* yaitu hukum yang berlaku adalah akibat utama perbuatan itu terjadi dan memberikan dampak kerugian bagi negara yang bersangkutan. Asas *Nationality* adalah hukum berlaku berdasarkan kewarganegaraan pelaku, Asas *Passive Nationality* adalah hukum berlaku berdasarkan kewarganegaraan korban, Asas *Protective Principle* adalah berlakunya berdasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya dan Asas *Universality* adalah yang berlaku untuk lintas negara terhadap kejahatan yang dianggap sangat serius seperti pembajakan dan terorisme (*crime against humanity*). Apabila hukum pidana Indonesia yang berlaku, maka terhadap pelaku penyebaran Virus dan Trojan Horse tersebut dapat dikenakan Pasal 33 dan Pasal 30 ayat (2) UU ITE.

DAFTAR PUSTAKA

Literatur :

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

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

Aloysius Wisnubroto, *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*, Yogyakarta : Universitas Widyatama, 1999.

Andi Hamzah, *Hukum Acara Pidana Indonesia*, Jakarta : CV Sapta Arta Jaya, 1996.

Asril Sitompul, *Hukum Internet, Pengenalan Mengenai Masalah Hukum di Cyberspace*, PT Citra Aditya Bakti, Bandung, 2001.

Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan*, PT.Raja Grafindo Persada, Jakarta, 2001.

Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Kajian Cyber di Indonesia*, Rajawali Pers, 2005.

Hinca IP Panjaitan dkk. *Membangun Cyberlaw Indonesia Yanng Demokratis*, IMLPC, Jakarta. 2005.

Hermawan Sulistyo Sutanto, dan Tjuk Sugiarto (Ed), *Cyber Crime Motif dan Penindakan*, Pensil 324, Jakarta.

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

I Wayan Parthiana, *Hukum Pidana Internasional*, Yrama Widia, Bandung.

Jujun S. Suriasumantri, *Ilmu Dalam Perspektif Moral, Sosial, dan Politik*, PT. Gramedia, Jakarta, 1986.

Merry Magdalena, dan Maswigrantoro Roes Setiyadi, *Cyberlaw, Tidak Perlu Takut*, C.V Andi Offset, Yogyakarta, 2007.

Munir Fuady. *Teori Hukum Pembuktian (Pidana dan Perdata)*. Citra aditya Bhakti. Jakarta. 2006.
M. Yahya Harahap. *Pembahasan Permasalahan dan Penerapan KUHAP Penyidikan dan Penuntutan*. Sinar Grafika. Jakarta. 2003.
P.A.F. Lamintang, *Dasar-Dasar Hukum Pidana Indonesia*, PT.Citra Aditya Bakti, Bandung, 1996.
Sultan Remy Syahdeini, *Kejahatan dan Tindak Pidana Komputer*, PT. Pustaka Utama Grafiti, Jakarta, 2009.
Tubagus Ronny Rahman, *Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi, Peradaban*, Jakarta, 2001.
Naskah Akademik RUU TI, UNPAD-DITJEN POLTEL DEPHUB, 2000.

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

Badan Pembinaan Hukum Nasional, Perkembangan Pembangunan Hukum Nasional tentang Hukum Teknologi dan Informasi, BPHN Departemen Kehakiman RI 1995/1996.

Peraturan Perundang-undangan :

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 48 Tahun 2009 Tentang Pokok-Pokok Kekuasaan Kehakiman.

Makalah, Jurnal :

AR Budi, *Aspek Perlindungan Hukum Nasabah dalam Sistem Pembayaran Internet.* Artikel dalam Jurnal Hukum. No 16.

Didi Widayadi, *Kebijakan dan Strategi Operasional Polri dalam kaitan hakikat ancaman Cybercrime*, makalah pada seminar Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, 29 Juli 2000.

Arief Muliawan, *Penegakan Hukum Tindak Pidana Informasi dan Transaksi Elektronika (cybercrime)*, disampaikan dalam seminar sehari dalam ranngka sosialisasi Undang-Undang Nomor 11 Tahun 2008 di Medan.

Koran :

Suara Merdeka, dengan judul *Reserse Polda Jateng Ungkap Kejahatan Internasional Internet*, 17 Nopember 2000.

Kompas, Berita Kompas Cyber Media (19/3/2002) 12 April 2002.

Website :

http://id.wikipedia.org/wiki/Sejarah_Internet

http://id.wikipedia.org/wiki

http://idfl.org/showthread.php?t=81197/Sejarah Internet di Indonesia

http://www.kejahatan dunia maya asal ketik.com.mht/dunia maya

http://www. Man 3 Malang.com/jenis-jenis kejahatan internet.mht

http://www.Ebisnionline.com/kejahatan internet;spamming.mht

http://www. Crouniclesofinhed.com/kejahatan computer.mht

http://www.symantec.com/norton/security_response/malware.jsp

http://www.isekolah.org/r_it_detail.php?itemid=h_1090285469

http://www.crime-research.org/library/Cyber-terrorism.htm

http://www.sinar harapan.com.mht/Indonesia peringkat ke-2 dunia kejahatan TI

http://www.missingkids.com/missingkids/servlet/PageServelt?PageId=1504

http://www.kejahatan dunia maya asal ketik.com.mht/dunia maya

http://www.maswiq@internews.or.id/GIPI-ASI@ ITC-APJII PEG-Cybercrime seminar/urgensi cybercrime law sebagai pelindung bagi pengguna teknologi informasi

http://www.nesl.edu/lawrev/vol37/1/marler.pdf, Marler, Sara L. *The Convention on Cyber-Crime: Should the United States Ratify?*

http://deluthus.blogspot.com/2011/02/8-contoh-kasus-cyber-crime-yang-pernah.html

http://freezcha.wordpress.com/2011/02/27/contoh-kasus-cybercrime-bagian2/

Tersedia di online : http://ejournal.unitomo.ac.id/index.php/hukum
E-ISSN : 2580-9113
P-ISSN : 2581-2033
LEX JOURNAL : KAJIAN HUKUM & KEADILAN

http://freezcha.wordpress.com/2011/02/27/contoh-kasus-cybercrime-bagian1/
http://freezcha.wordpress.com/2011/02/28/contoh-kasus-cybercrime-bagian3/