BAB I

PENDAHULUAN

A. Latar Belakang

Melihat perkembangan sejarah manusia, manusia sebagai *homo socius* (manusia sosial) diberikan kemampuan untuk berkomunikasi dalam mengatasi lingkungannya. Sejarah mencatat bahwa manusia tradisional telah menggunakan lambang-lambang isyarat sebagai alat komunikasi. Sekitar lima ratus tahun sebelum masehi, Darius, Raja Persia menempatkan prajuritnya di setiap puncak bukit kemudian mereka saling berteriak satu sama lain untuk menyampaikan informasi. Sementara itu, bangsa Indian dapat berkomunikasi pada jarak puluhan mil dengan teknik hembusan asap. Bentuk tulisan yang pertama kali digunakan adalah *piktograf* (berupa gambar kehidupan/perilaku pada dinding goa) dari orang Sumeria (3000 SM) yang sesungguhnya berupa gambar benda yang tampak sehari-hari. Lama-kelamaan *piktograf* berubah menjadi *ideograf* (berupa gambar yang mengandung penjelasan) yang mampu menyatakan gagasan. Selanjutnya, simbol-simbol yang dapat menggambarkan bunyi mulai muncul sampai pada akhirnya menjadi abjad modern. Penggunaaan *piktograf* berupa *milestone* komunikasi tulisan yang berkembang semakin cepat dengan ditemukannya *pa-pyrus* (kertas tulis pertama) yang memungkinkan terjadinya komunikasi jarak jauh dengan media surat, baik yang diantar dengan menggunakan jasa pelari, burung merpati, kuda, maupun kereta api. Penemuan

mesin cetak di China pada abad ke-10, yang disempurnakan oleh Johannes Guttenberg pada tahun 1440, kemudian mengantarkan manusia untuk mengenal media komunikasi massa cetak atau surat kabar pada abad ke-17[1]. Kemajuan teknologi informasi terus meningkat pesat hingga abad ini.

Perkembangan dan kemajuan teknologi informasi seiring dengan berjalannya waktu terus meningkat. Globalisasi menyebabkan perkembangan teknologi semakin pesat yang meliputi berbagai bidang dan aspek kehidupan manusia, seperti; ekonomi, politik, sosial, budaya, pertahanan dan keamanan, agama, serta hukum, hal ini sangat mempengaruhi kehidupan masyarakat pada umumnya. Kemajuan teknologi pada saat ini hampir sebagian besar telah dirasakan oleh penduduk Indonesia terutama bagi orang-orang yang sehari-harinya berhubungan dengan dunia teknologi informasi.

Kemajuan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi itu sendiri. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet[2]. Kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (*real*) ke realitas baru yang bersifat maya (*virtual*). Realitas yang kedua ini biasa dikaitkan dengan internet dan *cyber space*[3].

---

[1] Judhariksawan, *Pengantar Hukum Telekomunikasi*, Raja Garafindo Persada, Jakarta, 2005, hlm. 1-2

[2] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, Refika Aditama, Jakarta, 2005, hlm. 103

[3] *Loc.Cit.*

Pada saat ini komputer telah tersebar di kantor-kantor dan rumah-rumah termasuk juga ruko yang bergerak dalam bidang jasa internet. Di dunia barat pada era tahun 80-an, manusia mulai mengenal teknologi informasi dan pada era 90-an sudah mulai digunakan di seluruh dunia. Manusia telah dimanjakan oleh produk teknologi sehingga dengan mudah dapat mengunjungi belahan dunia lain dari yang kita tempati dan menjalin komunikasi secara global, atau bergabung dengan orang lain, belanja *online*, bahkan belajar menjadi teroris, menjadi anggota jaringan mafia, atau menjadi anggota kejahatan lainnya. Beberapa tahun terakhir banyak ditemukan tindak kejahatan melalui internet dengan menggunakan teknik yang sangat tinggi. Hal ini menimbulkan permasalahan yang sangat besar mengenai dampak dari internet yang dapat disalahgunakan.

Globalisasi ini membawa dua akibat dan makna dimana pada satu sisi globalisasi melahirkan dunia tanpa batas, menimbulkan keunggulan dibidang teknologi. Sementara di sisi lain globalisasi dapat juga menimbulkan dampak negatif untuk sebagian orang dengan memanfaatkan teknologi sebagai cara, alat atau sarana untuk melakukan tindak kejahatan melalui internet. Kemajuan teknologi yang merupakan hasil budaya manusia disamping membawa dampak positif, dalam arti dapat didayagunakan untuk kepentingan umat manusia juga membawa dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J. E. Sahetapy menyatakan, bahwa kejahatan erat kaitannya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Ini berarti semakin tinggi tingkat

budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat, dan cara pelaksanaannya.[4]

Perkembangan Internet yang semakin hari semakin meningkat, baik perangkat maupun penggunaannya, membawa dampak positif atau pun negatif. Dampak positif dari perkembangan internet banyak manfaat dan kemudahan yang kita dapatkan dari teknologi ini, sedangkan dampak negatif dari perkembangan internet melahirkan kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan menjadi lebih canggih melalui penggunaan media komputer secara *online* dengan risiko terdeteksi oleh pihak yang berwajib yang sangat kecil[5].

Dunia perbankan melalui internet (*e-banking*) Indonesia dikejutkan oleh tindakan seseorang bernama Steven Haryanto, seorang *cracker* dan jurnalis pada majalah Master Web. Ia dengan sengaja membuat situs yang menyerupai layanan internet banking Bank Central Asia (selanjutnya disebut BCA). Ia membeli *domain-domain* dengan nama mirip www.klikbca.com (situs asli Internet banking BCA), yaitu *domain* wwwklik-bca.com, kilkbca.com, clikbca.com, klickca.com, dan klikbac.com. Isi situs-situs ini hampir sama. Apabila nasabah BCA salah mengetik situs BCA asli maka nasabah tersebut masuk perangkap situs tiruan yang dibuat oleh Steven sehingga identitas pengguna (*user id*) dan nomor identitas personal dapat diketahuinya. Banyak nasabah BCA kehilangan datanya. Menurut pengakuan Steven, tujuan membuat situs tiruan ini adalah

---

[4] Ibid, hlm.26.

[5] Petrus Reinhard Golose*, Perkembangan Cyber Crime dan Upaya Penanggulangannya di Indonesia Oleh Polri*, Buliten Hukum Perbankan dan Kebanksentralan, Jakarta, Volume 4 Nomor 2, Agustus, 2006, hlm. 29-30

agar masyarakat pengguna internet berhati-hati dan tidak melakukan kesalahan saat melakukan pengetikan alamat situs (*typo site*), bukan untuk mendapatkan keuntungan. Contoh kasus lain adalah *cracker* bernama Dani Hermansyah, pada tanggal 17 April 2004 melakukan *deface* (perusakan) dengan mengubah nama-nama partai yang ada dengan nama-nama buah dalam *website* www.kpu.go.id yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap pemilu yang sedang berlangsung pada saat itu. Selain nama-nama partai yang diubah bukan tidak mungkin angka-angka jumlah pemilih yang masuk di sana menjadi tidak aman dan dapat diubah. Kelemahan administrasi dari suatu website juga terjadi pada penyerangan terhadap *website* www.golkar.or.id milik partai Golkar. Serangan terjadi hingga 1577 kali melalui jalan yang sama tanpa adanya upaya menutup celah disamping kemampuan *cracker* yang lebih tinggi. Dalam hal ini teknik yang digunakan oleh *cracker* adalah PHP *Injection* (bahasa *script* yang ditambahkan bersama HTML dan dapat dijalankan disamping server) dan mengganti tampilan muka *website* dengan gambar yang kurang pantas. Berdasarkan realitas tindak kejahatan di atas dapat dikatakan bahwa dunia ini tidak lagi hanya melakukan perang secara konvensional tetapi juga telah memasuki perang informasi. Menurut Peter Stephenson dalam bukunya yang berjudul *Investigating Computer –Related Crime*, perang informasi adalah usaha untuk mengakses, mengubah, mencuri, dan menghancurkan suatu sistem komputer.

Dewasa ini muncul kasus *botnet* (*robot network*) yang modus dan caranya dianggap sebagai *revolusioner* dari dunia *cyber crime*. *Botnet* ini dapat

menyebabkan suatu dampak negatif yang sangat besar, bahkan dapat mengarah pada *cyber terrorism*. Hal ini disebabkan tindak pidana *cracking* melaui *botnet* dapat mengendalikan lebih dari satu juta komputer oleh pelakunya. Oleh karena itu permasalahan yang baru muncul ini dianggap sangat berbahaya dan masyarakat dunia pun sibuk membahas penanganan dari serangan *botnet* ini.

Melihat fenomena di atas timbul persoalan, apakah hukum pidana positif kita dapat menjangkau kejahatan yang terjadi di dunia *cyber* atau dunia maya mengingat teknologi internet yang membentuk *realitas virtual* merupakan sesuatu yang baru sementara Kitab Undang-Undang Hukum Pidana (KUHP) adalah masa lalu dimana saat dibuat belum mengenal komputer apalagi internet, perdebatan terjadi diantara para pakar hukum.[6]

Sebagian berpendapat sesungguhnya kejahatan yang berkaitan dengan dunia *cyber*, pada dasarnya adalah sama dengan kejahatan biasa. Pada prinsipnya kejahatan yang berkaitan dengan dunia *cyber* adalah kejahatan konvensional, sama dengan kejahatan yang diatur dalam KUHP.

Sementara sebagian lain berpendapat bahwa minimal perlu pembaharuan hukum pidana atau lebih maksimal lagi, perlu undang-undang atau peraturan tertentu yang berkaitan dengan kejahatan dunia maya (*cyber*). Hal ini dikarenakan pada kenyataannya, dengan menggunakan instrumen hukum pidana yang telah ada, ternyata kejahatan di dunia *cyber* atau *cyber*

[6] Agus Raharjo, *Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Citra Aditya Bakti, Bandung, hlm. 56.

crime masih sulit untuk ditanggulangi bahkan cenderung semakin meningkat, kompleks dengan variasi modus operandinya.

Hal ini sangat *kotradiktif* (berlawanan) dengan kedudukan hukum sebagai sarana pembangunan sosial, dalam hal ini diharapkan posisi hukum berada di depan pembangunan, sehingga tidak asing lagi apabila dalam beberapa kasus tertentu di Indonesia, akibat dari seringkali muncul permasalahan dalam penggunaan teknologi, dan akibat permasalahan ini tersebut hakim mengalami kesulitan dalam memutuskan. Perbuatan diatas dapat dikategorikan sebagai tindak pidana cracking menggunakan botnet. Tindak pidana *cracking* ini merupakan suatu penggabungan dari beberapa teknik yaitu diantaranya membuat virus SASSER, melakukan serangan DoS (*Deniel of Service*) ke sebuah web, *The Trojan Horse,* berbagai teknik yang digabungkan sehingga dapat menciptakan suatu zombie (*botnet*) misal teknik XSS (*Cross site scripting*) dan beberapa teknik lainya seperti IP Soofing, Land Attack, Pink of Death, Syn Attack, Echo Spoof, UDP Flooding dengan target sistem komputer.

Di Indonesia telah diberlakukan peraturan perundang-undangan yang baru yang diharapkan dapat mengatasi berbagai permasalahan yang timbul akibat kemajuan zaman dan teknologi, termasuk tindak pidana *cracking* menggunakan *botnet* yakni Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun demikian, pada kenyataanya undang-undang tersebut seringkali tidak dapat mengakomodasi kasus-kasus tindak pidana *cracking* menggunakan *botnet* yang terjadi.

Dunia *cyber* adalah merupakan dunia tanpa batas dimana seseorang dapat pergi ke belahan dunia manapun dengan waktu yang singkat. Permasalahan yang muncul adalah ketentuan hukum yang dapat diterapkan kepada pelaku sementara modus yang dilakukan berbagai macam dan proses pembuktian kasus *cyber crime* yang tempat kejadian perkaranya di dalam dunia *virtual* terlebih suatu *cyber crime* dilakukan oleh tersangka di suatu negara terhadap korban di negara lain, begitu pula sebaliknya. Berdasarkan latar belakang di atas, maka Penulis mencoba melakukan penelitian hukum dengan mengambil judul penulisan : **"TINJAUAN HUKUM MENGENAI TINDAK PIDANA *CRACKING* MENGGUNAKAN *BOTNET* (ROBOT NETWORK) TERHADAP SISTEM KOMPUTER DIHUBUNGKAN DENGAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK"**

B. Identifikasi Masalah

Berdasarkan uraian di atas, maka pemasalahan yang timbul adalah sebagai berikut:

1. Bagaimana Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur mengenai tindak pidana *cracking* menggunakan *botnet* terhadap sistem komputer ?
2. Bagaimana upaya pembuktian atas tindak pidana *cracking* menggunakan *botnet* ?

C. Maksud dan Tujuan Penelitian

Adapun maksud dan tujuan dari yang dilakukan oleh penulis adalah sebagai berikut:

1. Untuk mengkaji dan menganalisis bagaimana Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur mengenai tindak pidana *cracking* menggunakan *botnet* terhadap sistem komputer.
2. Untuk mengkaji dan menganalisis bagaimana upaya pembuktian atas tindak pidana *cracking* menggunakan *botnet*.

D. Kegunaan Penelitian

Adapun kegunaan penelitian yang dilakukan oleh penulis adalah :

1. Secara teoritis

   Untuk mengetahui seberapa besar dampak kemajuan teknologi terhadap tindak pidana *cracking* menggunakan *botnet* serta penegakan hukum tindak pidana *cracking* menggunakan *botnet.*
2. Secara Praktis

   Hasil penulisan diharapkan dapat memberikan masukan bagi para pihak yang berwenang serta para penegak hukum dalam pengawasan hukum terhadap tindak pidana *cyber crime* yang berkembang pesat.

E. Kerangka Pemikiran

Salah satu tujuan pembangunan nasional Indonesia adalah untuk meningkatkan kesejahteraan warga negara Indonesia secara adil dan berkelanjutan, sesuai amanat alinea kedua Pembukaan Undang-Undang Dasar 1945. Secara prinsip prikeadilan adalah upaya untuk menemukan keadilan yang mutlak, serta merupakan manifestasi upaya manusia yang merindukan adanya hukum yang lebih tinggi dari hukum positif.[7]

Pembukaan Undang-Undang Dasar 1945 alinea kedua menyebutkan bahwa:

> "dan perjuangan pergerakan kemerdekaan Indonesia telah sampailah kepada saat yang berbahagia dengan selamat sentosa menghantarkan rakyat Indonesia ke depan pintu gerbang kemerdekaan negara Indonesia, yang merdeka, bersatu, berdaulat, adil dan makmur".

Makna yang tersirat dari kata adil dan makmur dalam alinea kedua tersebut merupakan keadilan yang diperuntukkan bagi seluruh rakyat Indonesia. Dimana hukum harus mampu memberikan manfaat. Dengan kata lain, seberapa besar hukum mampu malaksanakan atau mencapai hasil-hasil yang diinginkan, karena hukum dibuat dengan penuh kesadaran oleh negara demi tujuan tertentu.

Selain itu juga pelaksaan tujuan negara yang diamanatkan dalam alinea keempat Pembukaan Undang-undang Dasar 1945 yang menyatakan bahwa:

---

[7] Otje Salman Soemadiningrat dan Anton F.S, *Teori Hukum Mengingat, Mengumpulkan, Dan Membuka Kembali,* Refika Aditama, Bandung, 2004, hlm.156.

> “Kemudian dari pada itu untuk membentuk suatu pemerintahan negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, …”.

Pembukaan alinea keempat, menjelaskan tetang Pancasila terdiri dari lima sila. Pancasila secara substansial merupakan konsep yang luhur dan murni, luhur karena mencerminkan nilai-nilai bangsa yang diwariskan turun temurun dan abstrak. Murni karena kedalaman substansi yang menyangkut beberapa aspek pokok, baik agamis, ekonomi, ketahanan, sosial dan budaya, yang memiliki corak partikular[8].

Amanat dalam alinea keempat Pembukaan Undang-Undang Dasar 1945 tersebut merupakan konsekuensi hukum yang mengharuskan pemerintah tidak hanya melaksanakan tugas pemerintah saja, melainkan juga dalam alinea keempat merupakan landasan perlindungan bagi seluruh rakyat Indonesia, karena kata melindungi mengandung asas perlindungan hukum bagi segenap bangsa Indonesia untuk mencapai keadilan.

Tindak pidana *cracking* menggunakan *botnet* yang modus dan caranya dianggap sebagai *revolusioner* (cenderung menghendaki perubahan yang menyeluruh dan mendasar) dari dunia *cyber crime*. *Botnet* ini dapat menyebabkan suatu dampak negatif yang sangat besar, bahkan dapat mengarah pada *cyber terrorism*. Hal ini disebabkan tindak pidana *cracking* menggunakan *botnet* dapat mengendalikan lebih dari satu juta komputer oleh

[8] *Ibid*, hlm.158

pelaku. Oleh karena itu permasalahan yang baru muncul ini dianggap sangat berbahaya bertentangan dengan nilai-nilai yang ada dalam Pembukaan Undang-Undang Dasar 1945 alinea kedua dan keempat.

Cracking merupakan kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang *hacker* dan *cracker* dimana *hacker* sendiri identik dengan perbuatan negatif, padahal *hacker* adalah orang yang memiliki keahlian untuk mempelajari, menganalisa, dan selanjutnya bila menginginkan, bisa membuat, memodifikasi, atau bahkan mengeksploitasi kelemahan sistem perangkat lunak di komputer; biasanya kemudian dipublikasikan secara terbuka di Internet agar sistem menjadi lebih baik, sedangkan *cracker* adalah orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang di masuki seperti merusak data, pencurian data, penghapusan, dan banyak yang lainnya. Berdasarkan pengertian di atas, maka cracking sendiri merupakan suatu tindak pidana yang terdapat dalam lingkup hukum pidana.

Seiring dengan perkembangan *cracking*, muncul teknik yang sangat membahayakan pengguna internet yaitu *botnet* (robot network). Berbahaya karena jenis *cracking* ini dapat mengendalikan komputer yang sengaja terinfeksi oleh *bot herder* sehingga *bot-bot* tersebut tidak dapat dikendalikan oleh pemiliknya. *Botnets* adalah istilah untuk kumpulan komputer yang terinfeksi dengan kode-kode kejahatan yang dapat dikendalikan dari jarak jauh melalui

infrastruktur perintah dan kendali (*collections of computers infected with malicious code that can be controlled remotely through a command and control infrastructure*); *Bots* adalah komputer yang terinfeksi dengan kode kejahatan yang berpartisipasi dalam suatu botnet dan menjalankan perintah dari pengendali *botnet* (*individual computer infected with malicious code that participates in a botnet and carries out the commands of the botnet controller*); *Bot Herder* adalah seseorang yang memberi perintah dan mengendalikan beberapa kelompok *bots*, biasanya untuk suatu keuntungan (*A person that commands and controls groups of bots, often for profit*)[9].

Cracking mengunakan *botnet* terhadap sistem komputer merupakan perusakan yang dilakukan *cracker* terhadap sistem komputer melalui suatu teknik-teknik khusus. Tujuan pokok dari sistem komputer adalah mengolah data untuk menghasilkan informasi. Supaya tujuan pokok tersebut berjalan, maka harus ada elemen-elemen yang mendukungnya. Elemen-elemen dari sistem komputer adalah *software, hardware* dan *brainware. Cracking* menggunakan *botnet* inilah merusak salah satu dari sistem komputer yaitu *software*. *Software* (perangkat lunak/peranti lunak) adalah program yang berisi perintah-perintah untuk pengolahan data.

Cracking menggunakan *botnet* terhadap sistem komputer jelas merupakan suatu tindakan hukum yang ada dalam lingkungan ranah pidana. Pidana sendiri ialah suatu ketentuan hukum yang terdapat dalam Kitab Undang-Undang Hukum Pidana (KUHP). Namun perbuatan *cracking* menggunakan

[9] Mustrundie.wordpress.com/…/b-o-t-n-e-t-s-ancaman-dan-tantangan-ke-depan/, 4, Mei, 2010, 09.00 WIB

botnet itu sendiri belum diatur dalam KUHP. Hal ini dikarenakan KUHP merupakan produk hukum yang sudah lama. Diperlukan peraturan yang baru yang sesuai dengan perkembangan zaman di era globalisasi ini. Untuk itulah maka pemerintah mensahkan dan memberlakukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik demi tuntutan zaman dan demi menutupi segala kekurangan yang ada dalam KUHP yang sudah ketinggalan zaman walaupun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini sendiri dirasa belum mampu mengimbangi perkambangan *cyber crime* yang semakin pesat.

Berdasarkan Pasal 1 angka 3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> “Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi”.

Teknologi merupakan suatu perkembangan, kemajuan atau pembaharuan dari sederhana ke modern, informasi sendiri merupakan suatu hubungan komunikasi berupa berita. Teknologi informasi adalah teknik dimana memerlukan suatu keterampilan dalam suatu penggunaanya.

Dalam pasal ini menerangkan bahwa pengertian dari teknologi informasi yang berhubungan dengan tindak pidana *cracking* menggunakan *botnet* merupakan pemanfaatan teknologi informasi berbasis komputerisasi dimana di dalamnya terdapat suatu dokumen yang disimpan dalam bentuk elektronik.

Berdasarkan Pasal 1 angka 4 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> "Dokumen Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya".

Dokumen elektronik merupakan suatu simpanan, catatan atau bisa disebut juga bukti catatan yang diproses melalui media elektronik khususnya komputer.

Teknologi informasi yang berbasis komputerisasi ini menyimpan suatu dokumen yang berbentuk elektronik yang pada umumnya bersifat *personal* (rahasia) dan tidak dipublikasikan dan/atau diakses untuk umum. Pemanfaatan teknologi informasi berdasarkan suatu kepentingan yang positif dan iktikad baik. Namun dalam hal ini *cracking* menggunakan *botnet* merupakan suatu pemanfaatan teknologi yang bernilai negatif dan sangat merugikan dan berdampak sangat luas.

Berdasarkan Pasal 3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> "Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi".

Asas kepastian hukum berarti landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan. Asas manfaat berarti asas bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat. Asas kehati-hatian berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun bagi pihak lain dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik. Asas iktikad baik berarti asas yang digunakan para pihak dalam melakukan Transaksi Elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut. Asas kebebasan memilih teknologi atau netral teknologi berarti asas pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

Tindak pidana *cracking* menggunakan *botnet* merupakan suatu pelanggaran atas pasal tersebut. *Cracking* merupakan tindak pidana *cyber crime* yang menggunakan teknologi dan teknik yang sangat tinggi. Pihak penegak hukum sering terlambat dalam mengungkap kasus *cyber crime*. Ini disebabkan sulitnya mendapatkan bukti yang cukup. *Cracker* merupakan seseorang yang mempunyai kemampuan tinggi di bidang IT sehingga mampu mengelabui pihak berwajib. Contohnya, *cracker* menggunakan salah satu teknik yang disebut

teknik XSS (*cross site scripting*) dengan cara mencuri *cookies* seseorang dan menggunakannya sebagai *id* pelaku sehingga pihak yang berwajib tidak mampu mendeteksinya[10].

Pasal 32 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, menyebutkan :

> "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".

Adapun unsur-unsur yang terdapat dalam pasal tersebut adalah :

Unsur subjektif (dari dalam diri pelaku)

1. Dengan sengaja dan tanpa hak atau melawan hukum;

   Dengan sengaja dan tanpa hak adalah tindakan yang dilakukan oleh pelaku kejahatan telah direncanakan atau diniatkan terlebih dahulu dan tanpa sepengetahuan dari orang yang berhak serta telah melanggar ketentuan perundang-undangan.

Unsur objektif (dari luar pelaku)

1. Setiap Orang;

   Orang adalah orang perseorangan, baik warga Negara Indonesia, warga negara asing, maupun badan hukum.

2. Dengan cara apa pun;

[10] www.cert.org.id/-budi/courses/ec7010/2004/setyorini-report.doc, 4, Mei, 2010, 09.08 WIB

Dengan menghalalkan segala cara termasuk cara melalui pemanfaatan teknologi.

3. Informasi Elektronik dan/atau Dokumen Elektronik;

   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. Sedangkan Elektronik adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

4. Milik orang lain atau milik publik;

   Kepemilikannya merupakan bukan milik pelaku.

Pelaku memasuki, merusak, mengubah, dan menyebabkan tidak dapat dikendalikan sistem komputer di sebuah rumah sakit dengan melawan hukum.

Pasal ini dapat memenuhi unsur dari tindak pidana *cracking* menggunakan *botnet* terhadap suatu sistem komputer.

Berdasarkan Pasal 33 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> “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”.

Adapun unsur-unsur yang terdapat dalam pasal tersebut adalah :

Unsur subjektif (dari dalam diri pelaku)

1. Dengan sengaja dan tanpa hak atau melawan hukum;

   Dengan sengaja dan tanpa hak adalah tindakan yang dilakukan oleh pelaku kejahatan telah direncanakan atau diniatkan terlebih dahulu dan tanpa sepengetahuan dari orang yang berhak serta telah melanggar ketentuan perundang-undangan.

Unsur objektif (dari luar pelaku)

1. Setiap orang;

   Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
2. Melakukan tindakan apa pun;

Dengan menghalalkan segala cara termasuk cara melalui pemanfaatan teknologi.

3. Berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya;

   Yang dapat menyebabkan suatu akibat negatif terhadap system elektronik. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

Pada penegakan hukum materil, diperlukan hukum formil dalam mendukung proses penegakan dalam hukum tersebut. Maka, berdasarkan Pasal 5 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> “Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah”.

Pada kasus ini terdapat barang bukti informasi elektronik. Pada proses pembuktian suatu perkara, dalam kasus ini dapat ditempuh dengan menggunakan beberapa alat bukti yang harus diungkapkan pada persidangan, termasuk alat bukti PC milik tersangka.

Pasal 5 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> “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”.

Menurut Pasal 5 ayat (1) dan (2), Informasi Elektronik dan/atau Dokumen Elektronik dapat dijadikan alat bukti berdasarkan Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP) yang merupakan perluasan dari alat bukti Petunjuk sebagai alat bukti yang sah. Berdasarkan ketentuan tersebut dalam proses pembuktian, Dokumen Elektronik dan/atau hasil cetaknya merupakan perluasan dari alat bukti yang sah yang dapat diungkapkan pada persidangan yang berlaku dalam hukum acara di Indonesia. Tindak pidana *cracking* menggunakan *botnet* dapat dijerat dengan beberapa pasal yang ada dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Tindak pidana *cracking* menggunakan *botnet* terhadap suatu sistem komputer dapat mengakibatkan gangguan dan tidak terkendalinya suatu sistem komputer dan merupakan suatu kerugian besar yang berakibat buruk. Sehingga harus adanya keamana yang dijamin oleh Negara sebagaimana terdapat dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ini.

Berdasarkan Pasal 40 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> “Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan”.

Pemerintah dalam hal ini tidak hanya eksekutif saja, tetapi juga legislatif dan yudikatif pun harus ikut berperan dalam melindungi kepentingan umum. Kepentingan umum disini adalah segala sesuatu yang berhubungan dengan masyarakat dengan kaitanya dalam masyarakat informasi sehingga tercipta ketertiban umum yang dijamin dalam perundang-undangan.

Pihak kepolisian menjunjung tinggi hukum materil dan formil serta melakukan tugasnya guna menindak secara langsung, cepat, dan tepat sasaran dengan didukung instansi-instansi terkait dan masyarakat itu sendiri tentunya senhingga teercipta suatu keamanan, ketertiban dan keselarasan dalam berkomunikasi secara berkesinambungan agar tercipta suatu globalisasi yang sehat dan dinamis.

Pada dua dokumen Konferensi PBB mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal, yaitu *cybercrime* dan *computer related crime*. Dalam *background paper* untuk lokakarya Konferensi PBB X/2000 di Wina, Austria istilah *cybercrime* dibagi dalam dua kategori.

Pertama, *cybercrime* dalam arti sempit disebut *computer crime*. Kedua, *cybercrime* dalam arti luas disebut *computer related crime*[11].

Pada usaha untuk menanggulangi *cybercrime*, Resolusi Kongres PBB VIII/1990 mengenai *Computer Related Crimes* dan *International Industry Congres* (IIIC) 2000 *Millenium Congres* di Quebec pada tanggal 19 September 2000 dan Kongres PBB mengenai *The Prevention of Crime anda The Treatment of Offenders,* mengajukan beberapa kebijakan antara lain[12]:

1. Menghimbau Negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan computer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut:
   a. Melakukan modernisasi hukum pidana meteriil dan hukum acara pidana;
   b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
   c. Melakukan langkah-langkah untuk membuat warga masyarakat, aparat pengadilan dan penegak hukum sensitive terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer (*cybercrime*);
   d. Memperluas *rules of ethics* dalam penggunaan computer dan mengajarkannya dalam kurikulum informatika;

---

[11] Tim Perundang-undangan dan Pengkajian Hukum Direktorat Hukum Bank Indonesia, *Urgensi Cyberlaw Di Indonesia Dalam Rangka Penanganan Cybercrime Di Sektor Perbankan,* kerjasama penelitian antara Bank Indonesia dan Universitas Gajah Mada, Yogyakarta, 2006, hal. 1

[12] Barda Nawawi Arif, *Dalam United Nations (Eighth UN Congress On The Prevention Of Crime And The Treatment Of Offenders Report)*, 1991, hal. 141.

e. Mengadopsi kebijakan perlindungan korban *cybercrime* sesuai dengan deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cybercrime*.

2. Menghimbau negara-negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cybercrime*.
3. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (*committee on Crime Preventon And Control*) PBB untuk :
   a. Menyebarluaskan pedoman dan standar untuk membantu Negara anggota menghadapi *cybercrime* di tingkat nasional, regional dan internasional;
   b. Mengembangkan penelitian dan analisa lebih lanjut guna menemukan cara-cara baru menghadapi problem *cybercrime* di masa depan;
   c. Mempertimbangkan *cybercrime* sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerjasama di bidang penanggulangan kejahatan.

Selain itu juga negara-negara yang tergabung dalam Uni Eropa *(Council of Europe)* pada tanggal 23 November 2001 di kota Budapest, Hongaria telah membuat dan menyepakati *Convention on Cybercrime* yang kemudian dimasukkan dalam *European Treaty Series* dengan Nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal 5 (lima) negara, termasuk paling tidak ratifikasi yang dilakukan oleh 3 (tiga) negara anggota

Council of Europe. Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal *(criminal policy)* yang bertujuan untuk melindungi masyarakat dari *cyber crime,* baik melalui undang-undang maupun kerjasama internasional. Konvensi ini dibentuk dengan pertimbangan-pertimbangan antara lain sebagai berikut :

1. Bahwa masyarakat internasional menyadari perlunya kerjasama antar Negara dan Industri dalam memerangi kejahatan cyber dan adanya kebutuhan untuk melindungi kepentingan yang sah dalam penggunaan dan pengembangan teknologi informasi.
2. Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Hal lain yang diperlukan adalah adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat.
3. Saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Azasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik Dan sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi/pendapat.

Cracker itu sendiri adalah kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian, tindakan anarkis begitu mereka mendapatkan akses. Biasanya kita sering salah menafsirkan antara seorang *hacker* dan *cracker* dimana *hacker* sendiri identik dengan perbuatan negatif, padahal *hacker* adalah orang yang memiliki keahlian untuk mempelajari, menganalisa, dan selanjutnya bila menginginkan, dapat membuat, memodifikasi, atau bahkan mengeksploitasi kelemahan sistem perangkat lunak di komputer; biasanya kemudian di publikasikan secara terbuka di internet sehingga sistem menjadi lebih baik, sedangkan *cracker* adalah orang yang mencari kelemahan sistem dan memasukinya untuk kepentingan pribadi dan mencari keuntungan dari sistem yang di masuki seperti: merusak data, pencurian data, penghapusan, dan banyak yang lainnya.

F. Metode Penelitian

1. Spesifikasi penelitian

   Spesifikasi penelitian yang dilakukan adalah secara deskriptif analitis, yaitu suatu metode penelitian yang dilakukan dengan cara melukiskan dan menggambarkan fakta-fakta baik data sekunder bahan hukum primer berupa peraturan perundang undangan yang berhubungan dengan tindak pidana *cracking* menggunakan *botnet,* data sekunder bahan hukum sekunder berupa doktrin atau pendapat

para ahli dan data sekunder bahan hukum tersier berupa data yang didapat melalui majalah dan artikel yang berhubungan dengan tindak pidana *cracking* menggunakan *botnet*.

2. Metode Pendekatan

   Metode pendekatan yang dilakukan adalah secara yuridis normatif, yaitu suatu metode yang mana hukum dikonsepsikan sebagai norma, kaidah, asas atau dogma-dogma. Penafsiran hukum yang dilakukan adalah penafsiran gramatikal yaitu penafsiran yang dilakukan terhadap kata-kata atau tata kalimat yang digunakan pembuat undang-undang dalam peraturan perundang undangan tertentu, selain itu dilakukan juga penafsiran sistermatis yaitu penafsiran yang dilakukan dengan cara menghubungkan kata-kata dalam suatu pasal dengan kata-kata dalam pasal lain, baik dalam peraturan yang sama maupun antara berbagai macam peraturan perundang-undangan.

3. Tahap Penelitian

   a. Studi Kepustakaan (*Library Research*)

      Penelitian ini dilakukan dengan mencari data sekunder berupa:

      1) Bahan hukum primer yaitu peraturan perundang undangan, antara lain:

         a) Undang-Undang Nomor 11 tahun 2008 tentang Informasi Transaksi Elektronik.

         b) Kitab Undang-Undang Hukum Acara Pidana

c) Peraturan perundang-undangan yang relevan dengan tindak pidana *cracking* menggunakan *botnet.*

2) Bahan hukum sekunder yaitu bahan hukum berupa doktrin atau pendapat para ahli hukum terkemuka.

3) Bahan hukum tersier yaitu bahan yang memberikan informasi informasi berupa artikel majalah, makalah serta brosur

b. Studi lapangan (*Field Research*)

Penelitian dilakukan dengan mengunjungi tempat kegiatan secara online sebagai data primer untuk melengkapi data sekunder.

4. Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui penelaahan data yang diperoleh dari perundang-undangan, buku buku teks, hasil penelitian, majalah, artikel dan lain-lain, serta wawancara dengan pihak-pihak yang terkait dan mengunjungi situs internet yang berhubungan dengan tindak pidana *cracking* menggunakan *botnet.*

5. Metode Analisis Data

Data yang diperoleh dianalisis secara yuridis kualitatif, yaitu peraturan perundang-undangan tidak boleh saling bertentangan, memperhatikan hirarki peraturan perundang-undangan dan berbicara tentang kepastian hukum, bahwa perundang-undangan yang berlaku benar-benar dilakuakn oleh para pihak penegak hukum. Disamping

itu, berdasarkan Pasal 5 ayat 1 Undang-Undang Nomor 48 tahun 2009 tentang Kekuasaan Kehakiman bahwa hakim wajib menggali, mengikuti dan memahami nilai-nilai hukum dan rasa keadilan yang hidup dalam masyarakat, digunakan pula hukum tertulis dan hukum tidak tertulis.

6. Lokasi Penalitian

   Lokasi penelitian dilakukan di:

   a. Perpustakaan:
      1) UNIKOM (Universitas Komputer Indonesia), Jalan Dipati Ukur Nomor 112 Bandung.
      2) UNPAD (Universitas Padjadjaran), Jalan Dipati Ukur Bandung.
   b. Situs-situs:
      1) www.kaskus.com
      2) www.wikipedia.com