I. PENDAHULUAN

A. Latar Belakang Masalah

Seiring semakin berkembangnya kemajuan teknologi telekomunikasi, media, dan informatika, telah melahirkan internet sebagai salah satu fenomena penting dalam kehidupan manusia. Keberadaan aplikasi internet telah membawa berbagai dampak positif bagi kehidupan kita. Internet telah menyediakan akses yang murah, cepat, dan dapat dilakukan setiap saat untuk mendapatkan berbagai informasi yang kita inginkan dari seluruh dunia. Namun selain telah memberikan dampak positif, internet juga dapat memberikan dampak negatif.

Aplikasi internet dapat beroperasi dengan menggunakan sistem Komputer. Tujuan pokok dari suatu sistem komputer adalah untuk mengolah data yang diperoleh guna menghasilkan suatu informasi (Edmon Makarim, 2003: 392). Sehingga penyalahgunaan komputer yang menyimpang dari tujuan pokok tersebut dapat menimbulkan apa yang disebut sebagai kejahatan komputer.

Menurut Andi Hamzah (cet.2 1990: 26), kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal, memperluas pengertian kejahatan komputer dengan mengemukakan bahwa.

> Kejahatan komputer adalah segala aktifitas tidak sah yang memanfaatkan komputer untuk tindak pidana. Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau ilegal merupakan suatu kejahatan. Menurutnya pula, kejahatan komputer bukanlah merupakan kejahatan baru, melainkan kejahatan biasa, karena masih mungkin diselesaikan melalui KUHP.

Kejahatan komputer yang menggunakan internet disebut dengan tindak pidana mayantara (*cybercrime*).

> Menurut Barda Nawawi, tindak pidana mayantara adalah teknologi komputer dengan menggunakan internet tidak hanya digunakan untuk kegiatan pemerintah, bisnis, maupun pendidikan, tapi juga digunakan dalam melakukan kejahatan yaitu sebagai alat pencurian, penipuan, pornografi, dan berbagai kejahatan lainnya kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet ini disebut dengan istilah *cybercrime*. Barda Nawawi Arief, (2000: 8)

Isi dalam *back ground paper* untuk lokakarya kongres PBB X/2000 di Wina Austria PBB tentang *The prevention of crime and the treatment of offenders* menyebutkan dua istilah yang di kenal sebagai *cybercrime* :

a. *Cybercrime* dalam arti sempit adalah *computer crime* :
   "any illegal behavior directed by means of electronic operation that target the security of computer system and the data processed by them"
   (tindakan ilegal apapun yang terarah dengan maksud untuk eksploitasi Elektronika yang menargetkan keamanan dari sistem komputer dan data yang telah diolah)
b. *Cybercrime* dalam arti luas adalah *computer related crime* :
   "*any illegal behavior committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network"*
   (segala tindakan ilegal apapun yang telah dilakukan sehubungan dengan penawaran sistem komputer atau sistem atau jaringan, mencangkup kepemilikan, penawaran atau distribusi informasi ilegal yang ditujukan untuk sistem komputer atau jaringan)

Ditegaskan dalam dokumen PBB X/2000 di Wina Austria bahwa *cybercrime* meliputi kejahatan yang dilakukan:

1. dengan menggunakan sarana-sarana dari sistem/ jaringan komputer;
2. didalam sistem/jaringan komputer; dan
3. terhadap sistem/jaringan komputer

Berdasarkan kejahatan diatas bahwa *cybercrime* jenis ke 1 dan ke 2 merupakan *cybercrime* dalam arti luas, sedangkan jenis ke 3 merupakan cybercrime dalam arti sempit. (http://en.pendis.depag.go.id/Jurnal/6.achmad_tahir.pdf., 8 Januari 2010: 21.00)

Menurut Muhammad Bagir (2005: 3) *computer crime* dengan *cybercrime* mempunyai perbedaan dalam pelaksanaannya, perbedaannya adalah :

> "bahwa tindak kejahatan *cybercrime* tersebut dilakukan dengan memanfaatkan teknologi komputer yang berhubungan dengan jaringan informasi publik yaitu internet. Kejahatan komputer (*computer crime*) fase awal yang timbul di antaranya adalah penyerangan sistem telepon dan jaringan atau pentransferan uang menggunakan perangkat elektronik. Karena komputer pada awalnya berpusat dan tidak terkoneksi, peluang terjadinya kejahatan komputer lebih terbatas berupa penyalahgunaan sistem otorisasi penggunanya. Akan tetapi pengertian ini berkembang lebih luas karena saat ini komputer telah terkoneksi dengan jaringan internet. Sehingga terdapat perbuatan yang lebih luas dari *computer crime*, yaitu *cybercrime*."

Cybercrime tidak terbatas pada kejahatan terhadap perangkat komputer saja, tetapi ada kejahatan yang memanfaatkan komputer saja, tetapi ada kejahatan yang memanfaatkan komputer untuk melakukan kejahatan lain. Dengan demikian kejahatan *cybercrime* ini dapat dilakukan dengan dua cara, yaitu :

1. Kejahatan terhadap komputer, yang bertujuan merusak atau menyerang sistem atau jaringan komputer ;
2. Kejahatan yang menggunakan komputer (internet) sebagai alat dalam melakukan kejahatan.

Pendapat Susan W. Brenner mengatakan bahwa *cybercrime* memang benar nyata dan berbeda dari metode kejahatan tradisional sehingga membutuhkan artikulasi hukum baru dan pembentukan teknik investigasi yang baru. Akan tetapi jika mengasumsikan bahwa perbutan *cybercrime* bukanlah fenomena baru melainkan tidak lebih dari pelaku yang menggunakan sistem elektronik untuk melakukan sesuatu yang melanggar hukum, dan suatu sistem elektronik hanyalah media yang digunakan untuk melakukan kejahatan tradisional, maka tidak perlu ada kategori khusus untuk *cybercrime* dan membuat peraturan baru untuk mengatasinya; hukum yang sudah ada seharusnya cukup untuk melakukannya. Sebab sesuguhnya aktivitas di internet dan akibat hukumnya tidak bisa dilepaskan dari manusia yang ada didunia nyata, sehingga aturan hukum tradisional seharusnya dapat pula digunakan untuk mengatur aktivitas tersebut. (Susan W. Brenner, 2001: 3)

Pada prinsipnya, perbuatan-perbuatan yang dilakukan pada penyalahgunaan komputer itu sebagian besar sudah diatur dan ditetapkan dalam pasal-pasal KUHP, yang membedakannya dengan delik lama dalam KUHP adalah alat atau sarana yang dipakai untuk melakukan perbuatan penyalahgunaan terbaru itu yakni dengan memanfaatkan peralatan komputer. Namun, mengingat karaktekristik aktivitas diinternet yang dilakukan secara virtual dan tidak mengenal batas-batas teritorial, muncul asumsi mengenai bisa dan tidaknya sistem hukum tradisional

mengatur aktivitas tersebut. Dengan demikian, masalah yang timbul sebenarnya bukan mengenai perlu atau tidaknya suatu aturan hukum mengenai aktivitas di internet, melainkan mempertanyakan eksistensi sistem hukum tradisional dalam mengatur aktivitas di internet. Ditambah lagi, cybercrime merupakan kejahatan yang terjadi di suatu sistem elektronik sehingga sulit dipastikan yuridiksi hukum negara mana yang berlaku terhadapnya. (Andi Hamzah, cet.2 1990: 29)

Cybercrime memiliki beberapa bentuk, yang pada umumnya merupakan bentuk kejahatan biasa, hanya saja mengalami perkembangan dengan menggunakan teknologi. Menurut Didik M. Arief Mansur dan Elisatris Gultom membagi jenis kejahatan yang termasuk dalam kategori *cybercrime*, sebagai berikut :

1. *Cyber-terrorism*
2. *Cyber-pornography*. Penyebaran *obscene materials* termasuk *pornography, indecent exposure,* dan *child pornography*
3. *Cyber-harassment*. Pelecehan seksual melalui *e-mail, websites,* atau *chat programs*
4. *Cyber-stalking*. *Crimes of stalking* melalui penggunaan komputer dan internet
5. *Hacking*. Penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum
6. *Carding (credit-card fraud).* Melibatkan berbagai macam aktivitas yang melibatkan kartu kredit. *Carding* muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum. (Didik M. Arief Mansur dan Elisatris Gultom, 2005: 26)

Berdasarkan bentuk tindak pidana *cybercrime* di atas dan mempersempit pembahasan, maka penulisan skripsi hanya difokuskan pada salah satu bentuk *cybercrime*, yaitu *Cyberterrorism* Secara umum pengertian *Cyberterrorism* adalah konvergensi dari terorisme dan *cyberspace* (Mohammad Iqbal, 2004: 402). Penyebutan terminologi *cyberterororrism*, yang terdiri dari kata *"cyber"* dan *"terrorism"*, pertama kali dikemukakan pada tahun 1980 oleh Barry C.Colin, seorang peneliti senior di *Institute for Security and Intelligence* di California. Akan tetapi sebenarnya tidak terdapat definisi standar mengenai apa yang dimaksud dengan *cyberterrorism*, karena terorisme sendiri masih terdapat definisi luas. (Mohammad Iqbal, 2004: 402)

Cyberterrorism dalam perkembangannya telah membangun organisasi dan mempunyai jaringan global dimana kelompok-kelompok terorisme konvensional yang beroperasi di berbagai Negara telah terhubung oleh suatu jaringan terorisme international. Hubungan ini dilakukan dengan menggunakan teknologi informasi berupa internet yang sifatnya menjangkau seluruh dunia terutama untuk menyebarkan pesan, menyebarkan ideologi, mengumpulkan dukungan bagi organisasi, perekrutan anggota, dan berkomunikasi dalam merencanakan suatu serangan nyata. Bahkan menggunakan teknologi informasi untuk menggalang dana untuk kegiatan terorisme.

Cyberterrorism menjadi aktual sejak terjadinya peristiwa di Indonesia, pada tanggal 12 dan 16 Agustus 2006 lalu, polisi telah menangkap dua tersangka *cyberterrorism* dalam pembuatan situs http:www.anshar.net. dua orang tesebut bernama Agung Prabowo alias Max Fiderman (24) pada 12 Agustus 2006, dan

Agung Setiadi (30) yang disebut oleh polisi sebagai contoh kasus *cyberterorrism*. Situs ini menyebarluaskan bahan-bahan peledak dan senjata. Selain juga menebarkan orasi Noordin M.Top serta skenario pelaku bom bunuh diri pada kasus Bom Bali I, tanggal 12 Oktober 2002, Bom Bali II tanggal 1 Oktober tahun 2005 (http://m.detik.com), 23 Januari 2010: 14.00). Setelah kejadian bom Bali 1 dan bom Bali 2, pada tanggal 25 Agustus tahun 2009 lalu Datasemen Khusus 88 Polisi Republik Indonesia menangkap satu orang tersangka *cyberterrorism* sebagai kurir pendanaan bagi pelaku bom bunuh diri di Hotel JW Marriott dan Ritz-Carlton melalui situs Arrahman (www.arrahmah.com) satu orang tersebut bernama Muhammad Jibril Abdul Rahman alias Muhamad Ricky pada kasus ini tersangka disebut sebagai *cyberterrorist*, yang berarti bahwa kejahatan yang dilakukannya adalah kejahatan *cyberterorrism* (http://m.detik.com, 23 Januari 2010: 14.15).

Namun istilah kejahatan *cyberterorrism* tidak terdapat dalam peraturan perundang-undangan pidana di Indonesia. Indonesia sebagai negara hukum (*rechtstaat*) memiliki kewajiban untuk melindungi harkat dan martabat manusia. Salah satu bentuk perlindungan negara terhadap warganya dari tindakan atau aksi *cyberterrorism* adalah melalui penegakan hukum, termasuk di dalamnya upaya menciptakan produk hukum yang sesuai. Upaya ini diwujudkan pemerintah dengan mengeluarkan analogi atau perumpamaan dan persamaan pasal-pasal yang ada di Undang-undang :

1. Kitab Undang-undang Hukum Pidana (KUHP) dan Kitab undang-undang hukum acara Pidana (KUHAP)

2. Undang-undang Nomor. 15 tahun 2003 tentang penetapan peraturan pemerintah pengganti undang-undang Nomor. 1 tahun 2002 tentang pemberantasan tindak pidana terorisme, menjadi undang-undang. Selain mengatur aspek materil juga mengatur aspek formil. Sehingga, undang-undang ini merupakan undang-undang khusus (*lex specialis*) dari Kitab Undang-undang Hukum Pidana dan Kitab Undang-undang Hukum Acara Pidana. Dengan adanya undang-undang ini diharapkan penyelesaian perkara pidana yang terkait dengan terorisme dari aspek materil maupun formil dapat segera dilakukan.
3. Undang-Undang Nomor.36 Tahun 1999 Tentang Telekomunikasi
4. Undang-Undang Nomor.11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Menurut T. Nasrullah (2008:3) Diperlukannya undang-undang ini karena pemerintah menyadari tindak pidana terorisme merupakan suatu tindak pidana yang luar biasa (*extraordinary crime*), sehingga membutuhkan penanganan yang luar biasa juga (*extraordinary measures*).

Tentu perlu diketahui apakah kegiatan *cyberterrorism* yang dilakukan oleh pelaku dalam kasus situs anshar dan situs arrahmah tersebut diatas termasuk dalam kategori *cyberterrorism*, karena terorisme yang dilakukan adalah bentuk terorisme konvensional, meskipun menggunakan bantuan teknologi komputer dalam melakukan aksinya. Sehingga sangat penting mengidentifikasikan apa yang dimaksud dengan *cyberterrorism*. Yang bertujuan agar tidak tejadi kesalahan dalam memprosesnya di depan hukum, terutama untuk melakukan Penegakan

hukum yang lebih tepat untuk *cyberterrorism*, apakah cukup tertampung oleh undang-undang terorisme yang kita miliki, ataukah perlu diadakan amandemen terhadap undang-undang tersebut, atau justru perlu ada undang-undang baru yang khusus mengatur mengenai masalah kejahatan internet, termasuk didalamnya *cyberterrorism*.

Berdasarkan kasus di atas, maka peneliti tertarik melakukan penelitian dengan judul: **Analisis Penegakan Hukum *Cyberterrorism* di Indonesia**

B. Permasalahan dan Ruang Lingkup

1. Permasalahan

Berdasarkan pada uraian di atas, maka yang menjadi pokok permasalahan dalam penulisan skripsi ini dapat dirumuskan sebagai berikut :

a. Bagaimanakah penegakan hukum terhadap *cyberterrorism* di Indonesia ?
b. Apakah yang menjadi faktor penghambat dalam penegakan hukum *cyberterrorism* di Indonesia?

2. Ruang Lingkup

Adapun ruang lingkup dari penulisan skripsi ini agar tidak menyimpang dari pokok permasalahan yang akan dibahas, maka penulis membatasi ruang lingkup pembahasan menurut ilmu hukum pidana dengan mengkaji pelaksanaan mengenai Penegakan hukum tentang Undang-undang yang berlaku mengenai *cyberterrorism* serta mengkaji faktor apa saja yang menjadi penghambat dalam Penegakan hukum *cyberterrorism* di Indonesia dari tahun 2005-2010.

C. Tujuan dan Kegunaan Penelitian

1. Tujuan Penelitian

Tujuan penulisan agar dapat mengetahui :

a. Penegakan hukum terhadap *cyberterrorism* di Indonesia berdasarkan peraturan perundang-undangan yang berlaku.
b. Faktor penghambat dalam Penegakan hukum *cyberterrorism* di Indonesia

2. Kegunaan Penelitian

Kegunaan penelitian ini meliputi kegunaan teoritis dan praktis, yaitu :

a. Kegunaan Teoritis

Secara teoritis kegunaan penelitian ini berguna untuk dapat memberikan sumbangan ilmu pengetahuan, khususnya ilmu pengetahuan hukum tindak pidana *cybercrime* dan menambah perbendaharaan kepustakaan hukum.

b. Kegunaan Praktis

Secara praktis penulisan ini berguna sebagai bahan pemikiran dan masukan bagi para aparat penegak hukum Polisi, Jaksa, Hakim, masyarakat yang bernaung pada hukum dan para pengguna fasilitas layanan internet.

D. Kerangka Teoritis dan Konseptual

1. Kerangka Teoritis

Kerangka teoritis adalah kerangka-kerangka yang sebenarnya merupakan abstraksi dari hasil pemikiran atau kerangka acuan yang pada dasarnya bertujuan untuk mengadakan kesimpulan terhadap dimensi-dimensi sosial yang relevan untuk penelitian. (Soerjono Soekanto 1986:24).

Melakukan Analisis (*content analysis*), adalah teknik untuk menganalisa tulisan atau dokumen dengan cara mengidentifikasi secara sistematik atau ciri atau karakter dan pesan atau maksud yang terkandung dalam suatu tulisan atau dokumen. (Sri Mamudji.2005:4)

Menurut Sudarto (1986: 35), bahwa sistem peradilan pidana melibatkan penegakan hukum pidana dalam bentuk yang bersifat :

a. Penegakan hukum preventif, usaha pencegahan kejahatan agar pelaku kejahatan tidak melakukan kejahatan.
b. Penegakan hukum represif, suatu tindakan yang dilakukan aparat penagak hukum dalam menangani suatu kejahatan.
c. Penegakan hukum kuratif, suatu penanggulangan kejahatan yang lebih menitikberatkan pada pencegahan tindakan terhadap orang yang melakukan kejahatan.

Menurut Soerjono Soekanto (2010: 8), faktor-faktor yang mungkin mempengaruhi penegakan hukum sehingga dampak positif atau negatifnya terletak pada:

1. Hukumnya sendiri, hukum disini akan dibatasi pada undang-undang
2. Penegak hukum, pihak yang menerapkan hukum.
3. Sarana atau fasilitas yang mendukung penegakan hukum
4. Masyarakat , lingkungan dimana hukum tersebut berlaku dan diterapkan.
5. kebudayaan, hasil karya, cipta, dan rasa yang didasarkan pada karsa manusia didalam pergaulan hidup.

Menurut Freidman (Achmad Ali.2002:7), agar hukum dapat ditegakkan dengan baik, maka harus dibangun berdasarkan tiga unsur, antara lain :

a. Struktur Hukum (*Legal Structure*)
   Struktur menurut Freidman kerangka atau rangkanya yang memberi semacam bentuk dan batasan terhadap keseluruhan. Di Indonesia maka yang dimaksud struktur kepolisian, kejaksaan, dan pengadilan. Oleh karena itu, struktur yang dimaksud disini adalah penegak hukum.
b. Substansi Hukum (*Legal Subtance*)
   Substansi merupakan hal kedua yang menjadi penentu tegaknya hukum dalam sebuah lingkungan sosial. Substansi ini dilanjutkan Freidman adalah aturan, norma, dan prilaku nyata manusia yang berada dalam suatu sistem.

c. Kultur Hukum (*Legal Culture*)
   Freidman menjelaskan bahwa kultur hukum adalah sikap manusia terhadap hukum dan system hukum kepercayaan, nilai, pemikiran serta harapan. Dengan kata lain, kultur hukum adalah suasana pemikiran sosial dan kekuatan sosial yang menentukan bagaimana hukum digunakan, dihindari atau disalahgunakan.

Menurut Simecca dan Lee (Romli Atmasasmita, 2005: 57), konflik sebagai paradigma studi kejahatan organisasi masyarakat menganut prinsip-prinsip sebagi berikut :

a. Masyarakat terdiri dari kelompok-kelompok yang berbeda
b. Terjadinya perbedaan penilaian dalam kelompok-kelompok tersebut tentang baik dan buruk
c. Konflik antara kelompok-kelompok tersebut mencerminkan kekuasaan politik
d. Hukum disusun untuk kepentingan mereka yang memiliki kekuasaan politik.
e. Kepentingan utama dari pemegang kekuasaan politik untuk menegakan hukum adalah menjaga dan memelihara kekuasaannya.

Prespektif Konflik tidak yakin bahwa konflik kepentingan dapat diselesaikan, bahkan model prespektif konflik menuduh bahwa sesungguhnya tidak ada penyelesaian , melainkan yang ada hanyalah ”paksaan”(*coercion*) dari pemegang kekuasaan politik kepada kelompok yang tak berdaya

Kongres PBB Ke-8 Tahun 1990 di Havana (Barda Nawawi, 2002: 45) antara lain ditegaskan bahwa strategi dalam menanggulangi kondisi yang menimbulkan kejahatan adalah

> ”aspek-aspek sosial dari pembangunan merupakan faktor penting dalam pencapaian sasaran strategis pencegahan kejahatan dan harus diberikan prioritas paling utama” (*the social aspects of development are an important factor in the achievement of the objective of the strategy for crime prevention and criminal justice in the context of development and should be given higher priority*).

Menurut Soerjono Soekanto (2010: 7), gangguan terhadap penegakan hukum terjadi apabila adanya ketidakserasian antara nilai-nilai yang berpasangan, yang menjelma didalam kaidah-kaidah bersimpang siur, dan pola prilaku tidak terarah yang mengganggu kedamaian pergaulan hidup.

Selain teori di atas penulis menambahkan menggunakan teori *Cyberterrorism* merupakan konvergensi dari terorisme dan *cyber space*. Penyebutan terminologi *cyberterrorism*, yang terdiri dari kata ”*Cyber*” dan ”*Terrorism*”, pertama kali dikemukakan pada tahun 1980 oleh Barry C. Colin, seorang peneliti senior di *Institute for Security* and *Intelligence* di California. (Mohammad Iqbal, 2004: 402)

2. Konseptual

Konseptual adalah suatu kerangka yang menggambarkan antara konsep-konsep khusus yang merupakan arti-arti yang berkaitan dengan istilah yang digunakan dalam penulisan atau apa yang diteliti. (Soerjono Soekanto 1986:132).

Pengertian pokok-pokok istilah yang akan digunakan sehubungan dengan obyek dan ruang lingkup penulisan sehingga mempunyai batasan yang jelas dan tepat dalam penggunaannya.

Adapun istilah serta pengertian yang dipergunakan dalam penulisan skripsi ini meliputi :

a. Analisa isi adalah teknik untuk menganalisa tulisan atau dokumen dengan cara mengidentifikasikan secara sistematik ciri atau karakter dan pesan atau maksud yang terkandung dalam suatu tulisan atau dokumen. (Sri Mamudji.2005:4)

b. Secara konsepsional inti dan arti penegakan hukum adalah kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan di dalam kaidah-kaidah yang mantap dan mengejawantah dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir, untuk menciptakan, memelihara, dan mempertahankan kedamaian pergaulan hidup. (Soekanto Soerjono, 2010: 5)

c. Secara umum pengertian cyberterrorism menurut *Federal Bureau Of Investigation* adalah suatu bentuk kegiatan terencana yang termotivasi secara politis yang berupa serangan terhadap informasi, sistem informasi, program komputer dan data sehingga mengakibatkan kerugian besar serta jatuhnya korban yang tak berdosa yang dilakukan oleh satu kelompok group atau perorangan.

   (*The premeditated, politically motive attack against information, computer system, computer program, and data which result in violence against noncombatant targets by subnational groups or clandestine agents*)

   Tidak semua serangan terhadap suatu komputer dikategorikan sebagai suatu bentuk cyberterrorism. Suatu kegiatan dapat disebut cyberterrorism ketika serangan dilakukan terhadap sistem jaringan komputer serta infrastruktur telekomunikasi milik pemerintah militer atau pihak lainnya yang data mengancam keselamatan hidup manusia. Dengan demikian, serangan terhadap suatu sistem tanpa motif politik tidak dikategorikan sebagai cyberterrorism. (Sutan Remy Syahdeini, 2009: 99)

d. Terorisme adalah tindakan yang melawan hukum dengan cara menebarkan terror secara meluas kepada masyarakat, dengan mengancam atau cara kekerasan, baik yang diorganisir maupun tidak, serta menimbulkan akibat

berupa penderitaan fisik dan/atau psikologi dalam waktu berkepanjangan, kejahatan terhadap kemanusiaan (*crime against humanity*). (Petrus Reinhard, 2009: 6)

e. Tindak pidana terorisme adalah Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan bermaksud untuk menimbulkan suasana terror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal, dengan cara merampas kemerdekaan atau hilangnya nyawa atau harta benda orang lain, atau untuk menimbulkan kerusakan atau kehancuran terhadap objek-objek vital yang strategis, atau lingkungan hidup, atau fasilitas publik, atau fasilitas internasional. (Pasal 7, Undang-undang Nomor 15 Tahun 2003).

E. Sistematika Penulisan

Agar memudahkan dalam membaca dan memahami isi dari skripsi ini, maka penulis menyusun kedalam lima bab, yang isinya mencerminkan susunan dan ciri sebagai berikut :

I. PENDAHULUAN

Merupakan bab yang isinya memuat latar belakang tentang tindak pidana *cyberterrorism,* dan uraian latar belakang tersebut kemudian disusun pokok yang menjadi permasalahan dalam penulisan selanjutnya serta memberikan batasan-batasan penulisan. Selain itu pada bab ini juga memuat tujuan dan kegunaan dari penelitian, kerangka teoritis dan konseptual, serta sistematis penulisan.

II. TINJAUAN PUSTAKA

Merupakan bab pengantar dalam pemahaman pada pengertian-pengertian umum serta pokok bahasan tentang penegakan hukum tindak pidana *cyberterrorism*.

III. METODE PENELITIAN

Pada bab ini menguraikan tentang metode-metode yang dipakai dalam penulisan skripsi ini yang menunjukan langkah-langkah dalam pendekatan masalah, langkah-langkah penelitian, sumber dan jenis data, prosedur pengumpulan data dan pengolahan data serta analisis data.

IV. HASIL PENELITIAN DAN PEMBAHASAN

Merupakan bab yang memuat hasil-hasil penelitian dan pembahasan serta jawaban dari bagaimana penegakan hukum *cyberterorrism* di Indonesia, dan faktor penghambat dalam penegakan hukumnya yang telah dilakukan oleh penulis.

V. PENUTUP

Bab ini merupakan bab penutup yang berisikan kesimpulan hasil penelitian yang telah dilaksanakan, selanjutnya terdapat juga saran penulis yang berkaitan dengan pokok permasalahan yang dibahas dalam skripsi ini.

DAFTAR PUSTAKA

Arief, Barda Nawawi, 2000. *Tindak Pidana Mayantara, Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: RajaGrafindo Persada.

_____, 2002. *Bunga Rampai Kebijakan Hukum Pidana*. Bandung: Citra Aditya Bakti.

Atmasasmita, Romli, 2005. *Terori Kapita Selekta Kriminologi*. Bandung: Refika Aditama.

Hamzah, Andi, 1990. *Aspek-aspek Pidana di Bidang Komputer*: Jakarta: Sinar Grafika.

Makarim, Edmon,. 2003. *Komplikasi Hukum Telematika.* Jakarta: RajaGrafindo.

Mansur, Didik M. Arief dan Elisatris Gultom, 2005. *Cyber law: Aspek Hukum Teknologi Informasi*: Bandung: Refika Aditama.

Nasrullah, T. *Sepintas Tinjauan Yuridis Baik Aspek Hukum Materil Maupun Formil Terhadap Undang-undang Nomor 15/2003 Tentang Pemberantasan Tindak Pidana Terorisme.* Makalah Pada Semiloka tentang "Keamanan Negara" yang diadakan oleh Indonesia Police Watch bersama Polda Metropolitan Jakarta Raya.

Sudarto, 1986. *Kapita Selekta Hukum Pidana*. Bandung: Alumni.

Wahid, Abdul dan Muhammad Labib, 2005. *Kejahatan Mayantara* (*Cybercrime*), (Bandung: Rafika Aditama).

Undang-Undang No. 8, LN. No. 76 Tahun 1981 *Tentang Hukum Acara Pidana (KUHAP).*

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

Undang-undang Nomor 15, LN. Nomor 45 Tahun 2003, TLN. No. 4284.*Tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme, Menjadi Undang-undang.*

http://www.anshar.net

http://www.Arrahmah.com

http://m.detik.com

Achmad Tahir, *Penegakan Hukum Cyber Crime Di Indonesia*, http://en.pendis.depag.go.id, 07-2009.