HARMONISASI KONVENSI *CYBER CRIME* DALAM HUKUM NASIONAL

Oleh:

Akbar Kurnia Putra[1]

Abstrak

Perkembangan teknologi informasi menimbulkan dampak positif dan negatif dalam kehidupan masyarakat. Salah satu dampak negatifnya adalah timbulnya kejahatan baru yang menggunakan komputer dan jaringannya, baik sebagai target kejahatan maupun sebagai alat atau sarana kejahatan (cyber crime). Pemerintah telah mengundangkan UU ITE sebagai upaya untuk menanggulangi kejahatan tersebut, dan mulai berlaku tahun 2008. Agar UU tersebut dapat efektif mencapai tujuan diberlakukannya, maka perlu dilakukan kajian sejauhmana penyusunan UU tersebut telah mengakomodir bentuk-bentuk cyber crime yang dikenal selama ini, baik dalam instrumen hukum internasional maupun yang terjadi dalam praktik kehidupan sehari-hari. Dari hasil kajian terlihat bahwa masih ada bentuk cyber crime yang belum diatur dalam UU ITE, di antaranya adalah spamming, yang tidak menimbulkan kerugian secara ekonomis namun menimbulkan gangguan dan perasaan tidak menyenangkan pada pihak korban. Di sisi lain pengaturan kerjasama antar penegak hukum maupun kerjasama internasional dalam UU masih membutuhkan pengaturan lebih lanjut, agar penerapan UU ini dapat efektif menanggulangi cyber crime yang seringkali bersifat lintas batas teritorial.

Kata Kunci : *Cyber Crime*

I. LATAR BELAKANG

Kejahatan dunia maya atau yang juga dikenal dengan *cyber crime* adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputermenjadi alat, sasaran atau tempat terjadinya kejahatan.[2]Dalam Kongres Perserikatan Bangsa-Bangsa (PBB) ke-10 di Wina Austria pada 10-17 April 2000, istilah *cyber crime* dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*. Kedua, *cyber crime* dalam arti

[1] Dosen Bagian Hukun Internasional Fak. Hukum Universitas Jambi.
[2]http://id.wikipedia.org/wiki/Kejahatan_dunia_maya, 20 Januari 2013, pukul 19.53 WIB.

luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut:

1. *Cyber crime in a narrow sense* (*computer crime): any legal behavior directed by means of electronic operations that targets the security of computer system and the data processed by them.*
2. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*

Instrumen Hukum Internasional publik yang mengatur masalah *cyber crime* yang saat ini paling mendapat perhatian adalah konvensi tentang kejahatan *cyber* (*Convention on Cyber Crime*) 2001 yang digagas oleh Uni Eropa. Konvensi ini meskipun pada awalnya dibuat oleh organisasi regional eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diakses oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan *cyber*. 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. Hal ini dilakukan dengan penuh kesadaran sehubungan dengan semakin meningkatnya intensitas digitalisasi, konvergensi, dan globalisasi yang berkelanjutan dari teknologi informasi, yang menurut pengalaman dapat juga digunakan untuk melakukan tindak pidana.

Walaupun kejahatan dunia maya atau *cyber crime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana peralatan komputer atau jaringan komputer digunakan untuk mempermudah ataumemungkinkan kejahatan itu

terjadi.[3] Kejahatan ini dapat dilakukan oleh seseorang dari suatu tempat yang sangat pribadi (kamar tidur misalnya) tapi menimbulkan kerugian pada seseorang, atau institusi di tempat lain, yang terpisahkan oleh jarak ribuan kilometer, bahkan seringkali bersifat lintas batas territorial. Dengan demikian kejahatan ini kemudian membawa sifat *transnational crimes,* yaitu kejahatan yang bersifat lintas batas teritorial (*transnational boundaries*).

Sebagai contoh salah satu bentuk *cyber crime* adalah *hacking* (yang pelakunya disebut *hacker*). *Hacking* adalah bentuk pertama dalam kejahatan ini (*first crime*) sebagaimana ditetapkan oleh kongres PBB ke-X di Wina tahun 2000. Hal ini disebabkan bentuk perbuatan ini merupakan sesuatu yang istimewa, karena mempunyai kelebihan dari bentuk *cyber crime* lainnya. Diantaranya adalah bahwa pelaku kejahatan ini sudah barang tentu dapat melakukan *cyber crime* lainnya. Berikutnya secara teknis imbas dari aktivitas *hacking* menghasilkan kualitas akibat yang lebih serius dibandingkan dengan bentuk *cyber crime* lainnya. Untuk menyebarkan gambar porno atau *cyber pornography,* orang tidak perlu kemampuan *hacking,* cukup kemampuan minimal internet.[4]

Dari berbagai unsur perbuatan yang terdapat dalam Pasal 167 ayat (1) dan (2) KUHP, timbul berbagai pertanyaan jika dikaitkan dengan perbuatan *hacking*. Pertanyaan tersebut adalah; apakah sistem komputer seseorang atau sebuah organisasi, atau *website* dalam jaringan komputer (internet) dapat dikategorikan sebagai objek yang diatur dalam Pasal 167 KUHP? Dengan kata lain, apakah dapat disamakan memasuki sistem komputer orang lain dengan memasuki pekarangan atau rumah orang lain? Apakah menyadap *password* dapat disamakan dengan menggunakan kunci palsu sebagaimana diatur dalam pasal tersebut? Untuk menjawab pertanyaan tersebut maka hakim harus melakukan penafsiran yang mendalam, yang penggunaanya dalam hukum pidana masih menimbulkan perdebatan.

Model penegakan hukum, yang membutuhkan penafsiran meluas seperti diatas menimbulkan ketidakpuasan dibanyak kalangan. Ketidakpuasan tersebut karena

[3] Widodo, *Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime,* Laksbang Mediatama, Yogyakarta, 2009, hal. 24.

[4] Agus Raharjo, *Op. Cit,* hlm 200.

perbedaan persepsi di antara penegak hukum yang menimbulkan diskriminasi dalam penegakan hukum, sampai kepada ancaman pidana dalam pasal-pasal KUHP yang tidak sebanding dengan tingkat kerugian yang ditimbulkan oleh *cyber crime.* Desakan kepada pemerintah untuk segera meregulasi bentuk kejahatan ini akhirnya terjawab ketika pemerintah bersama Dewan Perwakilan Rakyat (DPR) menyetujui untuk memberlakukan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Meski tidak secara khusus merupakan undang-undang tentang *cyber crime*, beberapa pasal dalam undang-undang tersebut mengatur tentang *cyber crime.*

II. RUMUSAN MASALAH

Berdasarkan latar belakang tersebut maka penulis menyusun rumusan masalah:

Bagaimanakah Harmonisasi Konvensi *Cyber Crime* Tahun 2001 Dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ?

III. PEMBAHASAN

A. *CYBER CRIME*

Dalam *background paper* lokakarya Kongres PBB X pada tahun 2000 juga memberikan definisi *cyber crime*, akan tetapi membagi definisi tersebut dalam *narrow sense* (*arti sempit*) dan *broader sense* (*arti Luas*), dimana :[5]

> *"Cybercrime in narrow sense is Any illegal behavior directed by means of elctronic operations that targets the security of computer systems and the data processed by them."*
> *"Cybercrime as a broader sense* adalah *Any illegal behavior commited by means of, or in relation to, a computer system or network, including such crimes is illegal possession, offering or distributing information by means of a computer system or network."*

Sedangkan menurut Goodman & Brenner[6], istilah "*cybercrime*", "*computer crime*", dan "*high-tech-crime*" seringkali digunakan secara bergantian untuk

[5] *Background Paper* Kongres PBB X untuk *Workshop on CrimesRelated to the computer network,* dokumen A/CONF.187/10, 3-2-2000*,* hal.5 dikutip dari Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia, PT. Rajawaligrafindo Persada, Jakarta, 2006,* hal.8.

[6] Marc D. Goodman dan Susan W. Brenner, *The Emerging Consensus On Criminal Conduct in Cyberspace*, hal 10. Diakses melalui situs

merujuk kepada dua kategori, dimana suatu perbuatan telah dianggap melawan hukum. Dua kategori itu adalah, pertama, komputer merupakan target bagi perbuatan pelaku. Dalam hal ini pelaku bisa melakukan akses secara illegal, penyerangan kepada jaringan (pembobolan) dan lain lain yang terkait dengan sistem pengamanan jaringan (*networking*). Kategori kedua adalah bahwa perbuatan tersebut mengandung maksud dan tujuan seperti layaknya kejahatan konvensional, misal pencurian, pemalsuan.

Sesuai sifat global internet, ruang lingkup kejahatan ini juga bersifat global. *Cyber crime* seringkali dilakukan secara transnasional, melintasi batas negara sehingga sulit dipastikan yuridikasi hukum negara yang berlaku terhadap pelaku. Karakteristik internet di mana orang dapat berlalu-lalang tanpa identitas *(anonymous)* memungkinkan terjadinya berbagai aktivitas jahat yang tak tersentuh hukum.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain:

1. *Unauthorized Access to Computer System and Service*
2. *Illegal Contents*
3. Data *Forgery*
4. *Cyber Espionage*
5. *Cyber Sabotage and Extortion*
6. *Offense against Intellectual Property*
7. *Infringements of Privacy*

Menurut *Convention on Cybercrime*, tindak pidana yang dapat digolongkan sebagai *cybercrime* diatur dalam Pasal 2-5, adapun jenis tindak pidana tersebut adalah :

<http://www.lawtechjournal.com/articles/2002/ 03_020625_goodmanberner.php>, pada tanggal 1 April 2013.

1. *Illegal Access*

Diatur dalam Pasal 2 *Convention on Cybercrime*, yang berbunyi :

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

Illegal access melingkupi pelanggaran dasar dari ancaman-ancaman yang berbahaya dari serangan terhadap keamanan data dan sistem komputer.[7] Perlindungan terhadap pelanggaran *illegal access* ini merupakan gambaran dari kepentingan organisasi atau kelompok dan orang-orang yang ingin mengatur, menjalankan dan mengendalikan sistem mereka berjalan tanpa ada ganguan dan hambatan.

2. *Illegal Interception*

Diatur dalam Pasal 3 *Cybercrime Convention*, yang berbunyi :

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."

Menyatakan tidak sah tindakan pencegatan atau menahan tanpa hak bentuk pemindahan data komputer yang dilakukan secara pribadi yang dilakukan melalui faximile, *email*, atau pemindahan *file*. Tujuan dari pasal ini adalah perlindungan atas hak atas kebebasan dalam komunikasi data. Pelanggaran ini hanya ditujukan terhadap pemindahan pribadi dari data komputer.

[7]Council of Europe, *Explanatory Report To The Convention on Cybercrime* (ETS No 185), poin ke 44.

3. *Data Interception*

Diatur dalam Pasal 4 *Cybercrime Convention* yang berbunyi :

1) *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
2) *A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.*

Ketentuan pengerusakan data menjadi tindak pidana bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program komputer sebagaimana dengan benda-benda berwujud. Sebagai contoh adalah memasukan kode-kode jahat (*malicous codes*), *Viruses*, dan *Trojan Horse* ke suatu sistem komputer merupakan pelangagaran menurut ketentuan pasal ini.[8]

4. *System Interference*

Diatur dalam Pasal 5 *Cybercrime Convention* berbunyi

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."*

Dalam Pasal 5 konvensi ini disebutkan bahwa *system interference* ditetapkan sebagai pelanggaran pidana apabila "*... when committed intentionally, the serious hindering without right of the functioning of a computer system…*", harus dilakukan dengan memasukkan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer.

Pengganguan terhadap sistem dijadikan sebagai tindak pidana bertujuan untuk mencegah *"…the serious hindering without right of the functioning of a computer system…"*[9]

[8]Keyser, .*loc cit*., hal 302.
[9]Keyser, .*loc cit*., hal 303.

5. Misuse of Device

Misuse of Device diatur dalam Pasal 6 konvensi ini adapun yang termasuk jenis kejahatan ini adalah pencurian ,penyediaan, penjualan dan distribusi dari data komputer yang diperoleh dari sebuah alat.[10] Pasal 6 berbunyi:

> *"1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*
> *a the production, sale, procurement for use, import, distribution or otherwise making available of:*
> *i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;*
> *ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and*
> *b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. "*

Adapun yang di maksud alat disini adalah *hardware* maupun *software* yang telah di modifikasi untuk mendapatkan akses dari sebuah komputer atau jaringan komputer. Contohnya apabila ada sesorang yang memasukkan *keylogger* dalam jaringan bank untuk mendapatkan data-data nasabah mulai dari alamat sampai ke *password* ATM dan data-data tersebut dijual, digunakan atau didistribusikan untuk kejahatan lain.

B. HARMONISASI KONVENSI CYBER CRIME DALAM HUKUM NASIONAL

Indonesia sebagai salah satu bagian dari negara bangsa di dunia, termasuk negara dalam daftar hitam *(blacklist)* dunia perdagangan melalui

[10]ITU, *loc.cit*, hal 152

internet *(e-commerce*). Hal ini disebabkan banyaknya penyalahgunaan jaringan internet, khususnya dalam pemesanan barang-barang melalui internet.[11] Kondisi ini merugikan Indonesia, khususnya dunia perdangangan melalui internet, karena transaksi internet menggunakan kartu yang dikeluarkan oleh pihak perbankan Indonesia langsung ditolak oleh pihak luar negeri.

European Convention on Cyber Crime merupakan konvensi tentang *cyber crime* yang disepakati oleh Negara-negara anggota Uni Eropa, namun konvensi ini terbuka bagi Negara lain di luar Uni Eropa untuk mengikutinya. Oleh karena banyak Negara yang mengikuti konvensi tersebut, maka isi perjanjian ini menjadi model bagi banyak pengaturan cyber crime di berbagai Negara. Oleh karenanya menjadi penting bagi Negara kita untuk merujuk konvensi ini sebagai salah satu pembanding bagi pengaturan *cyber crime* di Indonesia.

Berbagai bentuk perbuatan *cyber crime* dalam *European Convention on Cyber Crime*, yaitu:

1. Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan system computer, yaitu:
    a. Mengakses system computer tanpa hak (*illegal acces*);
    b. Tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*);
    c. Tanpa hak merusak data (*data interference*);
    d. Tanpa hak mengganggu system (*system interference*);
    e. Menyalahgunakan perlengkapan (*misuse of device*).
2. Delik-delik yang berhubungan dengan computer, pemalsuan, dan penipuan (*computer related pffences; forgery and fraud*);
3. Delik-delik yang bermuatan pornografi anak (*content-related offences, child pornography*);

[11] Ilhamd Wahyudi (2006). *Kebijakan Pidana Terhadap Kejahatan Mayantara.* Tesis. Program Pascasarjana Unand-Unri. Padang, hlm 5.

4. Delik-delik yang berhubungan dengan hak cipta (*offences related of infringements of copyrights*).

Berbagai perbuatan diatas menjadi sandaran untuk menilai pengaturan dalam UU ITE dan menilai sejauhmana terdapat harmonisasi hukum dalam pengaturan tersebut.

Pengaturan *cyber crime* yang mengelompokan berbagai perbuatan ke dalam 2 klasifikasi besar, kemudian dibagi lagi dalam beberapa kelompok berdasarkan pasal-pasal di atas, dipedomani oleh pembuat UU ITE. Hanya saja pembuat UU ITE tidak mengelompokkan perbuatan tersebut secara eksplisit sebagaimana terdapat dalam Konvensi tersebut. Lebih jelasnya pengaturan *cyber crime* dalam UU ITE adalah sebagai berikut:

1. *Indecent Materials/ Illegal Content* (Konten Ilegal)

   Setiap orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, pencemaran nama baik serta pemerasan, pengancaman serta yang menimbulkan rasa kebencian berdasarkan atas SARA serta yang berisi ancaman kekerasan (Pasal 27, 28, dan 29 UU ITE)
2. *Illegal Acces* (Akses Ilegal)

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau Sistem Elektronik milik orang lain dengan cara apapun untuk memperoleh Informasi elektronik serta melanggar, menerobos, melampaui atau menjebol sistem pengamanan (Pasal 30 UU ITE).
3. *Illegal Interception* (Penyadapan Ilegal)

   Setiap orang dengan sengaja dan tanpa hak melakukan intersepsi atas Informasi Elektronik dan/ atau Dokumen Elektronik dalam suatu Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan,

penghilangan, dan/ atau penghentian Informasi Elektronik dan/ atau Dokumen Elektronik yang sedang ditransmisikan (Pasal 31 UU ITE).

4. *Data Interference* (Gangguan Data)

   Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, atau mentransfer suatu Informasi Elektronik milik orang lain atau milik publik kepada Sistem Elektronik orang lain yang tidak berhak, sehingga mengakibatkan terbukanya suatu Informasi Elektronik dan/ atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya. (Pasal 32 UU ITE).

5. *System Interference* (Gangguan Sistem)

   Setiap orang dengan sengaja dan tanpa hak melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/ atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya (Pasal 33 UU ITE).

6. *Misuse of Devices* (Penyalahgunaan Perangkat)

   Setiap orang dengan sengaja dan tanpa hak memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan yang dilarang dan sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu, yang ditujukan agar sistem elektronik menjadi dapat akses dengan tujuan memfasilitasi perbuatan yang dilarang (Pasal 34 UU ITE).

7. *Computer Related Fraud and Forgery* (Penipuan dan Pemalsuan yang berkaitan dengan Komputer)

   Setiap orang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, penghilangan, pengerusakan Informasi Elektronik dan/ atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik

dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik (Pasal 35 UU ITE).

Sebagaimana umumnya UU di luar KUHP yang mengatur perbuatan dengan sanksi pidana, dalam UU ITE perumusan perbuatan dan sanksi pidana juga dicantumkan secara terpisah. Semua perbuatan yang dilarang dalam Pasal 27 sampai Pasal 35 di atas, diancam dengan sanksi pidana dalam Pasal 45-52.

Jika diteliti pengaturan *cyber crime* dalam UU ITE maka terlihat bahwa semua perbuatan yang direkomendasikan dalam *European Convention on Cyber Crime* telah diatur dalam UU ITE. Perbedaannya hanya pada tata letak atau urutan pengaturan berbagai perbuatan tersebut. Jika Konvensi memulai dengan perbuatan yang terkategori sebagai *cyber crime* dalam arti sempit (murni), maka pengaturan dalam UU ITE tidak mengikuti pola tersebut. Hal ini terlihat bahwa pasal pertama yang mengatur tentang *cyber crime* tersebut, justru mengatur perbuatan yang sebenarnya merupakan tindak pidana konvensional (ada dalam KUHP), hanya saja sekarang dilakukan dengan media komputer berikut jaringannya. Perhatikan Pasal 27 yang melarang perbuatan orang yang dengan sengaja atau tanpa hak mendistribusikan, mentransmisikan, atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memilik muatan yang melanggar kesusilaan, perjudian, pencemaran nama baik, ataupun pemerasan.

IV. PENUTUP

Jika diteliti pengaturan *cyber crime* dalam UU ITE maka terlihat bahwa semua perbuatan yang direkomendasikan dalam *European Convention on Cyber Crime* telah diatur dalam UU ITE. Perbedaannya hanya pada tata letak atau urutan pengaturan berbagai perbuatan tersebut. Jika Konvensi memulai dengan perbuatan yang terkategori sebagai *cyber crime* dalam arti sempit (murni), maka pengaturan dalam UU ITE tidak mengikuti pola tersebut.

Terdapat tiga pendekatan untuk mempertahankan keamanan di *cyberspace, pertama* adalah pendekatan teknologi, *kedua* pendekatan sosial

budaya-etika, dan *ketiga* pendekatan hukum. Upaya menanggulangi kejahatan dengan tujuan utama perlindungan masyarakat untuk mencapai kesejahteraan masyarakat secara garis besar dapat dibagi dalam dua jalur yaitu jalur penal dan non-penal. Upaya pemberantasan dengan jalur penal yaitu Penerapan Hukum Pidana (*criminal law application*), sedangkan jalur non-penal dengan pencegahan tanpa pidana (*prevention without punishment*), mempengaruhi pandangan masyarakat tentang kejahatan dan pemidanaan melalui mass media (*influencing views of society on crime and punishment/mass media*).

DAFTAR PUSTAKA

A. Buku

Mauna, Boer. *Hukum Internasional Pengertian Peranan dan Fungsi dalam Era Dinamika Global*, PT. Alumni, Bandung, 2011.

Rahardjo, Agus. *Cyber Crime: Pemahaman dan Upaya Penangulangan Kejahatan Berteknologi.* Citra Aditya Bhakti, Bandung,2002.

Soekanto, Soerjono dan Sri Mamudji, *Penelitian Hukum Normatif*, Rajawali Press, Jakarta, 2007.

Sujatmiko, Eko. *Kamus Teknologi Informasi Dan Komunikasi*, Aksara Sinergi Media*, Surakarta, 2012.*

Sukarni, *Cyber Law: Kontrak Elektronik dalam Bayang-bayang Pelaku Usaha,* Pustaka Sutra, Bandung, 2008.

Suparni, Niniek. *Cyberspace Problematika & Antisipasi Pengaturannya*, Sinar Grafika, Jakarta, 2009.

Widodo. *Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime,* Laksbang Mediatama, Yogyakarta. 2009.

B. Jurnal dan Internet

Romizal.*Prinsip Tanggung Jawab Negara atas Pengelolaan Lingkungan Hidup Menurut Hukum Internasional Dan Implementasinya Pada Peraturan Perundang-Undangan Di Indonesia*, Skripsi Sarjana Hukum Universitas Jambi, Jambi, 2003.

Claudia Chandra, Inggrid. Gaya Hidup Manusia, http://regional.kompasiana.com/2013/01/29/gaya-hidup-manusia--528988.html, 12 Januari 2013, pukul 15.00 WIB.

Nurrohman, M. Pengertian Internet adalah, http://caramembuatada.blogspot.com/2011/10/pengertian-internet-adalah.html, 12 Januari 2013, pukul 01.37 WIB.

http://id.wikipedia.org/wiki/Kejahatan_dunia_maya, 20 Januari 2013, pukul 19.53 WIB.

http://kbbi.web.id/, 11 Maret 2013, pukul 22.00 WIB.

http://id.wikipedia.org/wiki/Konvensi_Jenewa, 11 Maret 2013, pukul 22.30 WIB.

C. Peraturan Perundang-undangan

Convention on Cyber crime

Undang-Undang RI Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Eletkronik