PROSPEK KERJASAMA INTERNASIONAL DALAM PENANGANAN *CYBER CRIME*

Skripsi ini diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana pada Jurusan Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Hasanuddin

OLEH

RUSDIANSYAH HAERUS

E 131 05 048

UNIVERSITAS HASANUDDIN

MAKASSAR

2009

HALAMAN PENGESAHAN

JUDUL : PROSPEK KERJA SAMA INTERNASIONAL DALAM PENANGANAN *CYBER CRIME*

N A M A : RUSDIANSYAH HAERUS

N I M : E 131 05 048

JURUSAN : HUBUNGAN INTERNASIONAL

FAKULTAS: ILMU SOSIAL DAN ILMU POLITIK

Makassar, November 2009

Mengetahui

Pembimbing I,

Prof. Dr. J. Salusu, MA.
NIP. 130 100 374

Pembimbing II,

Drs. Aspiannor Masrie
NIP. 131 982 457

Mengesahkan

Ketua Jurusan,

Drs. Patrice Lumumba, MA.
NIP. 131 658 796

HALAMAN PENERIMAAN TIM EVALUASI

JUDUL : PROSPEK KERJA SAMA INTERNASIONAL DALAM PENANGANAN *CYBER CRIME*

N A M A : RUSDIANSYAH HAERUS

N I M : E 131 05 048

JURUSAN : HUBUNGAN INTERNASIONAL

FAKULTAS: ILMU SOSIAL DAN ILMU POLITIK

Telah diterima oleh Tim Evaluasi Sarjana Fakultas Ilmu Sosial dan Ilmu Politik Universitas Hasanuddin Makassar untuk memenuhi syarat-syarat guna memperoleh gelar sarjana pada Jurusan Ilmu Hubungan Internasional pada hari Sabtu, 14 November 2009

TIM EVALUASI

Ketua : Drs. Patrice Lumumba, MA .....

Sekretaris : Burhanuddin, S.IP., M.Si .....

Anggota : 1. Prof. Dr. Basir Syam .....

2. Drs. Aspiannor Masrie .....

3. Pusparida Syahdan, S.Sos., M.Si .....

KATA PENGANTAR

Alhamdulillah, penulis haturkan dihadapan Allah SWT, Sang Maha Pencipta dan Sang Pemberi Rahmat, Hidayah, Karunia, dan pertolongan, yang tentu bagi penulis adalah segalanya yang menjadi bagian dari skripsi ini.

Penulis sadar bahwa skripsi ini dalam berbagai hal adalah sebuah karya yang sederhana, bahkan jauh dari kesempurnaan. Dan skripsi ini mungkin diragukan validitasnya, adalah hak pembaca dalam menilainya. Oleh karenanya, penulis sangat terbuka akan pemikiran-pemikiran kritis yang bernilai konstruktif dari pembaca sekalian.

Terlebih dahulu penulis menghaturkan beribu terima kasih dari lubuk hati yang terdalam kepada keluargaku yang tercinta, ayahanda **Drs. H. Haerus** dan Ibunda **Hj. Hartati Dj. S.Pd** atas kasih sayang, doa, dan dukungannya dalam mengerjakan tugas ini serta *my true love* dan cahaya mataku **Wahyuningsih "Ayhu"** yang membuatku selalu semangat dengan kehangatan cintanya. Demikian pula dengan saudara-saudaraku **Titi, Nha-na, dan Aan.**

Penulis juga mengucapkan rasa terima kasih dan penghargaan yang dalam kepada Bapak **Prof. Dr. J. Salusu, MA** selaku **konsultan I** dan Bapak **Drs. Aspiannor Masrie** selaku **konsultan II** atas segala bimbingan dan arahan yang sangat berarti sejak awal hingga rampungnya penulisan skripsi ini. Rasa terima kasih yang dalam juga penulis khususkan kepada Seluruh Bapak dan Ibu Dosen HI atas segala transfer keilmuannya sejak penulis terdaftar sebagai mahasiswa Universitas Hasanuddin, serta Staff Akademik pada jurusan Ilmu Hubungan internasional khususnya **Bunda** dan **Bu Rahma** yang telah banyak membantu dalam menyelesaikan urusan-urusan akademik. Begitu pula pada Bapak dan Ibu di kantor Akademik pada Fakultas Ilmu Sosial dan Ilmu Politik atas segala kemudahan dan bantuannya yang besar dalam pengurusan kelengkapan administrasi penulis.

Melalui kesempatan ini pula, penulis juga ingin menyampaikan rasa terima kasih dan penghargaan kepada semua pihak yang telah membantu penyusunan skripsi ini sebagai berikut :

1. **Prof. Dr. dr. Idrus A. Paturusi,** Rektor Universitas Hasanuddin.
2. **Drs. Patrice Lumumba, MA**, Ketua Jurusan Ilmu Hubungan Internasional.
3. **Drs Aspiannor Masrie**, Sekertaris Jurusan Ilmu Hubungan Internasional.
4. Buat teman-teman se-angkatanku, **Regime 05 ; Alam, Ancu, Anto, Awal, Arqam, Amsal, Hidayat, Radis, Ibrahim, Tauhid, Herwin, Farid, Noe, Sahar, Imam, Ina, Maya, Rian, Audy, Novi, Eka, Mery, Fika, Dora, Icha, Ani, Nunu, Nino, Fina, Rika, Citra, Dea, Ana, Dian Amalia, Riri, Dewi, Heriani, Feby, Puthe', Murni, Dian, dan** semuanya yang tidak sempat saya sebutkan namanya.
5. Buat teman-teman se-angkatanku **Reguler Sore ; Viktor, Malik, Haris, Herman, Ikhsan, dan Mike** yang telah sama-sama berjuang dalam menyelesaikan skripsi ini.

Akhirnya dengan penuh kerendahan hati, penulis memohon maaf yang sebesar-besarnya bilamana terdapat hal-hal yang diluar kemampuan penulis selama mengikuti kuliah.

Makassar, Desember 2009

Rusdiansyah Haerus

ABSTRAKSI

Rusdiansyah Haerus, E13105048, dengan skripsi berjudul : "***Prospek Kerjasama Internasional dalam Penanganan Cyber Crime***", dibawah bimbingan **Prof. Dr. J. Salusu, MA** selaku pembimbing I dan **Drs. Aspiannor Masrie** selaku pembimbing II, Jurusan Ilmu Hubungan Internasional, Fakultas Ilmu Sosial Dan Ilmu Politik, Universitas Hasanuddin, Makassar.

Penulisan ini bertujuan untuk menggambarkan tentang prospek kerjasama internasional dalam penanganan *cyber crime*.

Metode penelitian yang digunakan dalam penulisan skripsi ini adalah tipe penelitian deskriptif, dimana penulis akan menggambarkan secara sistematis mengenai fakta-fakta yang terdapat dalam fenomena *cyber crime*. Dalam hal ini, penulis berusaha untuk menjelaskan dampak teknologi informasi terhadap timbulnya *cyber crime*, kendala-kendala berupa faktor – faktor pendorong dan penghambat dalam kerjasama penanganan *cyber crime*, dan menggambarkan prospek kerjasama internasional dalam penanganan *cyber crime*.

Dengan menggunakan telaah pustaka, yaitu pengumpulan data dengan menelaah sejumlah literatur yang berhubungan dengan masalah yang diteliti baik berupa buku-buku, artikel-artikel, majalah, surat kabar serta mengakses pusat media informasi seperti internet yang berhubungan dengan masalah yang diteliti. Dalam skripsi ini, penulis berusaha untuk menggambarkan upaya kerjasama internasional dalam penanganan *cyber crime*..

Hasil penelitian menunjukkan bahwa (1) Munculnya revolusi teknologi informasi dewasa ini dan masa depan terhadap timbulnya *cyber crime* hanya membawa dampak pada perkembangan teknologi itu sendiri dan juga akan mempengaruhi aspek kehidupan lain seperti agama, kebudayaan, sosial, politik, kehidupan pribadi, masyarakat bahkan bangsa dan negara. (2) Dalam mengatasi kendala-kendala berupa faktor-faktor pendorong dan penghambat dalam kerjasama penanganan *cyber crime* dapat dilakukan berupa bantuan teknis, pelatihan, penyediaan fasilitas sampai dengan pertukaran informasi yang diperlukan serta harmonisasi ketentuan-ketentuan hukumnya pada setiap negara. (3) Pengembangan mekanisme kerjasama internasional, baik dalam lingkup global, regional maupun bilateral harus terus dilakukan guna pencegahan dan penanggulangan kejahatan transnasional. Mengingat bahwa *cyber crime* tidak mengenal batas-batas negara maka dalam upaya penanggulangannya memerlukan suatu koordinasi dan kerjasama antarnegara. *Cyber crime* memperlihatkan salah satu kondisi yang kompleks dan penting untuk diadakannya suatu kerjasama internasional oleh karena kejahatan ini adalah merupakan salah satu kejahatan baru yang beraspek internasional dan global.

DAFTAR ISI

Halaman

DAFTAR TABEL

DAFTAR GAMBAR

UNIVERSITAS HASANUDDIN

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Hubungan Internasional merupakan suatu studi yang mempelajari interaksi berbagai aktor yang berbeda yang berpartisipasi dalam politik internasional, termasuk negara, organisasi internasional, organisasi non-pemerintah, kesatuan subnasional seperti birokrasi dan pemerintah lokal, serta individu. Studi hubungan internasional mencakup berbagai definisi dan aspek, meliputi : organisasi internasional, keamanan internasional, dan ekonomi politik global. Berbagai aspek dalam hal tersebut telah menjadi realitas yang melintasi batas-batas negara atau yang menyangkut negara yang berbeda. Jadi, Hubungan Internasional adalah suatu studi tentang kebiasaan aktor-aktor yang berpartisipasi baik secara individual maupun bersama-sama dalam proses politik internasional.

Terdapat beberapa aspek yang sering dibahas dalam studi hubungan internasional yaitu aspek globalisasi dan keamanan. Globalisasi adalah sebuah istilah yang memiliki hubungan dengan peningkatan keterkaitan dan ketergantungan antarbangsa dan antarmanusia di seluruh dunia. Sebagai contoh, globalisasi melalui perdagangan, investasi, perjalanan, budaya populer, dan bentuk-bentuk interaksi yang lain sehingga batas-batas suatu negara menjadi bias. Keamanan adalah suatu keadaan bebas dari bahaya. Sebagai contoh, keamanan fisik, informasi, finansial, dan komputer.

Dalam era globalisasi saat ini perkembangan terjadi sangat cepat seiring dengan peningkatan teknologi informasi. Globalisasi yang disertai dengan kemajuan teknologi komunikasi yang pesat menyebabkan hubungan antarbangsa, antarmasyarakat dan antarindividu semakin dekat, saling tergantung dan saling mempengaruhi sehingga tercipta suatu dunia tanpa batas (*borderless word*). Dengan demikian, kebutuhan akan informasi sudah menjadi hal vital yang sangat dibutuhkan oleh masyarakat di dunia.

Perkembangan teknologi informasi hampir terjadi pada setiap negara yang sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara (*borderless*). Keberadaan suatu teknologi informasi mempunyai arti dan peranan yang sangat penting di dalam aspek kehidupan. Hal ini membuktikan bahwa ketergantungan akan tersedianya teknologi informasi semakin meningkat, dimana teknologi informasi merupakan infrastruktur bagi perkembangan suatu negara.

Peningkatan kebutuhan informasi menyebabkan perkembangan yang spektakuler di bidang teknologi informasi yang terdiri dari teknologi elektronika, teknologi komputer, teknologi telekomunikasi dan teknologi penyiaran. Salah satu contohnya adalah internet yang mana hampir sejumlah 1,5 miliar manusia di dunia sudah terkoneksi dengan internet. Internet telah menciptakan dunia baru yaitu dunia komunikasi yang berbasis komputer yang menawarkan realitas baru yang berbentuk *virtual* (tidak langsung dan tidak nyata), namun pada pelaksanaannya komunikasi dilaksanakan secara nyata seolah-olah berada di tempat tersebut (*real time*) dan melakukan hal-hal nyata seperti bertransaksi dan berdiskusi.

Peningkatan teknologi informasi khususnya internet, selain memberi manfaat juga menimbulkan dampak negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Dampak ini terlihat dari adanya *cyber crime* (kejahatan dunia maya) yang terjadi di berbagai belahan dunia. *Cyber crime* kini merupakan salah satu fenomena baru dari kemajuan teknologi, dimana tindak kejahatan ini hingga sekarang sangat sulit untuk ditanggulangi. *Cyber crime* tergolong tindak kejahatan internasional, sesuai dengan hukum internasional yang menjelaskan tentang definisi tindak kejahatan internasional yaitu tindak kejahatan yang mempengaruhi prerogatif dan legitimasi beberapa atau semua negara yang mengakibatkan ancaman bahaya terhadap hubungan masyarakat internasional.[1] Jadi, *cyber crime* bukan hanya masalah nasional tapi juga masalah internasional.

Cyber crime (kejahatan dunia maya) merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi. Tindak kejahatan dunia maya atau *cyber crime* ini didasari atas motif yang beragam seperti motif ekonomi, politik, ideologi, agama, dan kriminal yang potensial menimbulkan kerugian bahkan perang informasi. Pelaku yang melakukan *cyber crime* biasa disebut dengan *hacker* yang berarti orang yang mempunyai kemampuan teknologi dan pemograman komputer yang mengakses sistem komputer yang mempunyai otorisasi dengan menggunakan sistem jaringan komputer lain untuk menggunakan data yang ada didalamnya.[2]

---

[1] G.I Tunkin, 1986, *International Law*, Progress Publisher : Moscow h. 361-362
[2] Encarta Dictionary Tools, 2003, Microsoft Corporation

Cyber crime sendiri memiliki berbagai macam interpretasi. Sering diidentikkan dengan *computer crime*. The U.S. Department of Justice memberikan pengertian *computer crime* sebagai : *"...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution"*. *Computer crime* pun dapat diartikan sebagai kejahatan di bidang komputer yang secara umum dapat diartikan sebagai penggunaan komputer secara illegal.[3] Dari beberapa pengertian di atas, *computer crime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai komputer sebagai sarana/alat atau komputer sebagai obyek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.[4] Secara ringkas *computer crime* didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi yang canggih.[5]

Bentuk atau aktifitas *cyber crime* dapat berupa *Cyber Sabotage and Extortion*, yakni kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.[6] Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Kejahatan ini sering disebut sebagai *cyber terrorism*.

---

[3] Andi Hamzah, *Aspek-Aspek Pidana di Bidang Komputer*, 1998. h. 2

[4] Ari Juliano Gema, 2000, *Cyber crime : Sebuah Fenomena di dunia Maya*, www.bisnisindonesia.com..

[5] Wisnubroto, 1999, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer*, Yogyakarta, h. 77.

[6] *Op. cit.*,

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya tersimpan dalam suatu sistem yang *computerized.*[7] Permasalahan yang ditimbulkan akibat perkembangan teknologi komputer dan informasi, menunjukkan perlu adanya upaya yang menyeluruh untuk menanggulangi *cyber crime*. Kesadaran dari para pengguna jasa internet terhadap *cyberethics* juga akan turut membantu. Selain itu, kerjasama antara negara-negara pengguna jasa internet juga membantu menanggulangi paling tidak mengurangi kejahatan internet yang melintasi batas-batas negara.

Cyber crime merupakan masalah internasional, maka diperlukan upaya hukum internasional dalam mengantisipasi masalah *cyber crime*. Perkembangan dalam hukum internasional sendiri memang telah menunjukkan bahwa telah dilakukan berbagai upaya hukum internsional dalam mengantisipasi *cyber crime*. Menurut Ahmad M. Ramli, instrumen hukum internasional di bidang *cyber crime* merupakan sebuah fenomena baru dalam tatanan modern mengingat *cyber crime* sebelumnya tidak mendapat perhatian dari negara-negara sebagai subyek hukum internasional.[8] Munculnya bentuk kejahatan baru yang tidak saja bersifat lintas batas tetapi juga terwujud dalam tindakan-tindakan virtual telah menyadarkan masyarakat

---

[7] Majalah Gatra edisi Oktober 2004, *Judul : Cybercrime di era digital*, website : http://www.gatra.com/2004-10-13/ diakses pada tanngal 25 Maret 2009

[8] Ahmad M. Ramli, *Perkembangan Cyber Law Global dan Implikasinya Bagi Indonesia*, Makalah Seminar *The Importance of Information System security in E-Goverrment*, Tim Koordinasi Telematika Indonesia, Jakarta, 28 Juli 2004, h. 5-6

internasional tentang perlunya perangkat hukum internasional baru yang dapat digunakan sebagai kaidah hukum internasional dalam mengatasi kasus-kasus *cyber crime*.

Adapun instrumen hukum Internasional yang dapat dirujuk dalam fenomena *cyber crime* sebagai kejahatan transnasional adalah *United Nations Conventions Againts Transnational Organized Crime*, atau yang dikenal dengan *Palermo Convention*, tahun 2000. Dalam *Palermo Convention* ini ditetapkan bahwa kejahatan-kejahatan yang termasuk dalam kejahatan transnasional adalah kejahatan narkotika, genocide, uang palsu, kejahatan di laut bebas, terorisme, perdagangan senjata api, korupsi, pornografi, perdagangan wanita dan anak-anak Internasional, pencucian uang dan cyber crime.[9] Dalam hal ini, permasalahan yang ditimbulkan akibat perkembangan teknologi komputer dan informasi, menunjukkan perlu adanya upaya yang menyeluruh untuk menanggulangi *cyber crime*.

Dari penggambaran singkat dampak *cyber crime* di atas maka dapat kita lihat betapa masalah ini menjadi isu global dalam masalah internasional, dimana tindak kejahatan ini tidak mengenal batas-batas teritori negara sehingga mampu menyerang negara manapun dan dapat melibatkan banyak negara. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas dari perkembangan *cyber crime* ini. Oleh karena itu, salah satu solusinya selain kesadaran dari para pengguna jasa internet terhadap *cyberethics* yang turut membantu adalah menciptakan kerjasama antara negara-negara pengguna jasa

[9] BisTek Warta Ekonomi No. 24 edisi Juli 2000, *Judul : jenis-jenis kejahatan komputer*, h. 52-54

internet yang juga turut membantu menanggulangi paling tidak mengurangi kejahatan internet yang melintasi batas-batas negara.

Pada dasarnya interaksi internet bersifat bebas dengan adanya *civil cyberliberty* dan pribadi (*privacy*). *Cyberliberty* dalam internet dipakai sebagai media yang efektif untuk melancarkan ancaman internet (*cyberthreat*). *Cyberliberty* juga memudahkan orang melakukan kejahatan yang merusak moralitas, nilai dan norma seperti perjudian, prostitusi maupun pornografi. Telah banyak contoh bentuk kejahatan yang terjadi di dunia maya, seperti kasus-kasus mafia *cyber* yang merebak pertengahan tahun 2004 di Amerika Serikat.[10] Lalu di Indonesia sendiri pernah mengalami, ketika sistem jaringan Komisi Pemilihan Umum (KPU) pada tahun 2004 disusupi oleh para *hacker*.[11]

Hal ini tentu saja mencemaskan karena ketika dunia semakin tergantung kepada teknologi dan manajemen berbasis pada informasi, ternyata kemajuan dalam penanggulangan kejahatan berbasis teknologi ini dapat dikatakan berjalan perlahan. Perlunya kerjasama keamanan tersebut telah menjadi suatu kajian yang ditujukan untuk membentuk penanggulangan *cyber crime* oleh nagara-negara secara bersama, terutama kerjasama internasional yang menyelenggarakan pengawasan dan pengontrolan *cyber crime*. Melalui kerjasama ini diharapkan dapat menggugah masyarakat internasional untuk ikut berpartisipasi dalam penanggulangan kejahatan berteknologi tinggi.

---

[10] FBI Tangkap Mafia *Cyber* , http://cybertech.cbn.net.id, diakses pada tanggal 02 Maret 2009

[11] Data Pemilu KPU Diserang "*Hacker*", www. Kompas.com edisi 08 Juli 2004, diakses pada tanggal 25 Maret 2009.

Melihat permasalahan di atas maka penulis tertarik untuk menganalisis masalah ini yang akan diangkat dalam skripsi yang berjudul " ***Prospek Kerjasama Internasional Dalam Penanganan Cyber Crime*** ".

B. Batasan dan Rumusan Masalah

Cyber crime merupakan salah satu bentuk kejahatan atau pelanggaran yang terjadi di dunia internet. Dimana tindak kejahatan ini tidak bisa dianggap sebagai masalah kecil di samping masalah-masalah kejahatan lainnya, disebabkan karena *cyber crime* bersifat global dan melintasi batas negara serta bentuknya terus berkembang pesat sejalan kemajuan teknologi. Indikasi yang menunjukan bahwa kemajuan teknologi ini terjadi salah satunya adalah makin banyaknya kelompok ekstrimis melakukan tindak kejahatan melalui internet. Sedangkan,

Hubungan Internasional merupakan suatu studi tentang persoalan-persoalan luar negeri dan isu-isu global di antara negara-negara dalam sistem internasional, termasuk peran negara-negara, organisasi-organisasi antar pemerintah, organisasi-organisasi non-pemerintah atau lembaga swadaya masyarakat, dan perusahaan-perusahaan multinasional. Dengan kata lain, hubungan internasional melibatkan aktor non–negara yang melintasi batas–batas teritorial suatu negara. Hubungan internasional mencakup rentang isu yang luas mulai dari globalisasi dan dampak-dampaknya terhadap masyarakat, kedaulatan negara sampai kelestarian ekologis, proliferasi nuklir, nasionalisme, perkembangan ekonomi, terorisme, kejahatan yang terorganisasi, keselamatan umat manusia, serta hak-hak asasi manusia

Dalam pembahasan masalah yang akan diteliti agar tidak terlalu luas maka penulis membatasi masalah yaitu pada "prospek kerjasama internasional dalam penanganan *cyber crime*" yang dimaksud adalah bagaimana harapan atau hambatan ke depan dalam menangani *cyber crime* melalui kerjasama internasional.

Berdasarkan pada batasan masalah tersebut di atas, maka masalah dapat dirumuskan sebagai berikut :

1. Bagaimana dampak kejahatan di Internet (*cyber crime*) sebagai kejahatan transnasional ?
2. Kendala-kendala apa saja yang dihadapi dalam kerjasama internasional khusunya dalam penanganan *cyber crime* ?
3. Bagaimana prospek kerjasama internasional dalam penanganan *cyber crime* ?

C. Tujuan dan Kegunaan Penelitian

1. Tujuan Penelitian

Penelitian ini dilakukan dengan tujuan :

a. Untuk mengetahui dampak kejahatan di Internet (*cyber crime*) sebagai kejahatan transnasional.
b. Untuk mengetahu kendala-kendala apa saja yang dihadapi dalam kerjasama internasional khusunya dalam penanganan *cyber crime.*
c. Untuk mengetahui prospek kerjasama internasional dalam penanganan *cyber crime.*

2. **Kegunaan Penelitian**

a. Penelitian ini diharapkan dapat memberikan informasi mengenai sejauh mana keterkaitan fenomena *cyber crime* dalam interkasi internasional.

b. Sebagai informasi yang dapat digunakan sebagai bahan pertimbangan terhadap pemerintah dalam penanggulangan kejahatan transnasional khususnya *cyber crime*.

D. Kerangka Konseptual

Untuk memperoleh gambaran sistematis tentang masalah pokok yang telah dikemukakan, maka penulis hendak mengemukakan konsep-konsep yang dipergunakan dalam menganalisa masalah ini secara umum. Dalam studi hubungan internasional terdapat sebuah kecenderungan dimana negara tidak lagi terbatas hanya berhubungan dengan satu negara saja (bilateral) melainkan lebih luas lagi menjadi hubungan dengan beberapa negara (multilateral), baik itu negara yang tergabung dalam sebuah organisasi regional ataupun lembaga internasional.

Tujuan sebuah negara melakukan hubungan internasional adalah untuk memenuhi kepentingan nasionalnya. Oleh sebab itu, negara tersebut perlu memperjuangkan kepentingan nasionalnya di luar negeri. Dalam melakukan perjuangan tersebut dibutuhkan suatu kerjasama untuk mempertemukan kepentingan nasional antar negara berupa kerjasama internasional. Kerjasama merupakan salah satu kegiatan dalam dan luar negeri yang dapat dilakukan oleh suatu negara demi tercapainya tujuan suatu negara tersebut. Dalam Hubungan Internasional, kerjasama

bisa dilakukan di dalam segala aspek kehidupan, diantaranya dalam bidang ekonomi, politik, sosial, budaya, pendidikan, keamanan dan aspek-aspek lainnya. Dengan adanya ketergantungan ini, maka secara otomatis akan menimbulkan suatu hubungan timbal balik antara negara kerjasama dalam bidang tertentu, yang nantinya akan saling menguntungkan masing-masing negara.

Kerjasama internasional adalah bentuk interaksi yang dilakukan antar negara-negara ataupun melibatkan aktor non-negara yang menyadari kesalingtergantungan yang mengelilingi mereka. Kerjasama internasional merupakan alat bagi aktor-aktor hubungan internasional yang fungsinya memfasilitasi dan melayani berbagai macam kegiatan yang tak ada batasnya. Kerja sama ini meliputi berbagai macam bidang seperti politik, keamanan, ekonomi, budaya dan sebagainya.

Sedangkan menurut Ernest B. Haas, kerjasama internasional adalah :

> Proses dimana aktor-aktor politik nasional dari berbagai negara diminta mengarahkan loyalitas, harapan, dan kegiatan politik mereka ke institusi pusat baru dan lebih besar; yang lembaga-lembaganya memiliki atau mengambil alih yurisdiksi yang semula berada di tangan negara bangsa.[12]

Holsti memberikan beberapa alasan mengapa negara-negara melakukan kerjasama internasional :[13]

- Untuk meningkatkan kesejahteraan ekonomi, melalui kerja sama negara-negara dapat memotong ongkos produksi untuk memenuhi kebutuhan mereka dan rakyatnya meskipun negara-negara tersebut mengalami keterbatasan baik dalam segi sumber daya alam maupun manusia.

---

[12] Jack C. Plano dan Roy Olton, *The Internatinal Relations Dictionary*, Clio Press Ltd, 1982, h. 331-332

[13] Kj Holsti, *The state, war, and the state of war,* Cambridge University Press, 1995, h. 362

- Untuk meningkatkan efisiensi, seperti pengurangan biaya dan ongkos.
- Karena adanya masalah-masalah yang mengancam keamanan bersama.
- Untuk mengurangi atau menghilangkan image negatif yang selama ini menjadi landasan bagi negara lain memandang negara tersebut.

Dengan menggunakan konsep kerjasama internasional maka penulis hendak menganalisis fenomena *cyber crime* khususnya prospek kerjasama internasional dalam penanganan *cyber crime* sebagai aspek yang melintasi batas-batas suatu negara.

Dalam masalah tersebut terdapat suatu kejahatan baru yang sangat berpengaruh terhadap berbagai aspek seperti aspek keamanan. Kejahatan ini adalah salah satu dampak dari proses globalisasi yang sedang berjalan saat ini, hal ini terjadi karena teknologi informasi yang semakin maju yaitu dengan adanya internet dan komputer. Seiring dengan perkembangan teknologi internet menyebabkan munculnya kejahatan yang disebut dengan "*cyber crime*" atau kejahatan melalui dunia maya.

Istilah *cyber crime* saat ini merujuk pada satu tindakan kejahatan yang berhubungan dengan dunia maya atau *cyber space* dan segala tindakan-tindakan kejahatan yang menggunakan media komputer dan internet. Ada ahli yang menyamakan antara tindak kejahatan di dunia maya (*cyber crime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan keduanya. Meskipun belum ada kesepahaman mengenai definisi kejahatan Teknologi Informasi (TI), namun ada kesamaan pengertian universal mengenai kejahatan komputer.

Secara umum yang dimaksud kejahatan komputer atau kejahatan di dunia maya adalah "Upaya memasuki dan menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut". Bila seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seijin yang berhak, tindakan tersebut sudah tergolong pada kejahatan komputer karena telah melanggar hak privasi orang lain.

Cyber crime telah menjadi salah satu aspek yang paling sering dibahas dalam studi hubungan internasional khususnya masalah keamanan internasional. Berdasarkan keterkaitan atas fenomena di atas, maka terdapat beberapa studi hubungan internasional yang menyangkut masalah fenomena *cyber crime* diantaranya yaitu keamanan internasional, hukum internasional, globalisasi, dan transnasional *crime*.

E. Metode Penelitian

1. Tipe Penelitian

Tipe penelitian yang penulis gunakan adalah deskriptif, dimana penulis akan menggambarkan secara sistematis mengenai fakta-fakta yang terdapat dalam fenomena *cyber crime* dan menganalisa prospek kerjasama internasional dalam penanganan *cyber crime*.

2. Teknik Pengumpulan Data

Teknik pengumpulan data yang akan dipergunakan oleh penulis dalam penelitian ini adalah telaah pustaka (*library research*) yaitu cara pengumpulan data

dari buku-buku, artikel, jurnal, dokumen, karya ilmiah, kamus, majalah, dan surat kabar elektronik yang berkaitan erat dengan masalah yang dikemukakan dalam tulisan ini. Data yang diperoleh adalah data sekunder. Penulis akan melakukan penelitian dari beberapa literatur yang berhubungan dengan permasalahan yang akan ditulis oleh penulis. Adapun tempat yang akan dikunjungi, yaitu :

- Perpustakaan UNHAS di Makassar
- Perpustakaan Pusat di Makassar

3. Teknik Analisis Data

Teknik analisis data yang dipergunakan penulis adalah teknik analisis kualitatif dimana data yang diperoleh dari berbagai literatur akan diinventarisasikan dan diklarifikasi kemudian permasalahan digambarkan berdasarkan fakta-fakta yang ada dan disusun dalam tulisan. Yang menjadi pokok analisis adalah prospek kerjasama internasional dalam penanganan *cyber crime*.

UNIVERSITAS HASANUDDIN

BAB II

TINJAUAN PUSTAKA

A. Teknologi Informasi Dalam Interaksi Transnasional

Dalam hubungan transnasional aktor non-negara memiliki peranan yang cukup besar dalam interaksi global yang terdiri dari komunikasi, keuangan, perjalanan dan keuangan. Aktor non-negara dapat bergerak secara bebas dalam melintasi batas-batas negara untuk melakukan kegiatannya, karena itu aktor non-negara inilah yang secara intensif melakukan hubungan transnasional tersebut. Hubungan yang dilakukan oleh negara itu dapat dinyatakan sebagai *interstate relations* dimana hubungan yang dilakukan oleh aktor non-negara lebih mengurusi bidang perekonomian, sedangkan hubungan yang dilakukan oleh negara lebih mengurusi bidang keamanan. Tetapi ada perbedaan dalam sistem internasional kontemporer, yaitu banyaknya interaksi aktor non-state yang telah mampu mempengaruhi dan menciptakan suatu peristiwa internasional yang disebut sebagai transnasionalisme. Oleh karena itu, peran negara sangat dibutuhkan dalam hubungan transnasional.

Rosenau mendefenisikan transnasionalisme sebagai :

> *"the process where by international relations conducted by governments have been supplemented by relations among private individuals, groups, and societies that can do have important consequences for the course of events."*[14]

---

[14] Paul R. Viotti dan Mark V. Kauppi, 1993, *International Relations Theory : Realism. Pluralism, Globalism*, Second Edition, New York : MacMilan Publishing Company, h. 239.

Menurut Rosenau, dalam transnasionalisme keberadaan aktor-aktor non negara seperti individu, kelompok, dan masyarakat bersifat hanya melengkapi keberadaan aktor negara. Selain itu, Rossenau juga menjelaskan bahwa keterlibatan aktor-aktor non negara dalam hubungan internasional memberikan pengaruh penting terhadap terjadinya suatu peristiwa internasional. Dalam konteks ini, keberadaan non negara dapat dilihat sebagai aktor apabila dalam interaksinya dengan non negara lain, ataupun dengan negara lain, mempunyai dampak terhadapa berlangsungnya suatu peristiwa.

Sementara menurut Kohane dan Nye, persoalan ada tidaknya pengaruh dari aktor transnasional terhadap suatu peristiwa transnasional bukan merupakan hal yang pokok. Mereka lebih menekankan pada aspek interaksi atau hubungan timbal balik yang berlangsung. Koehane dan Nye mengasumsikan bahwa :

> Interaksi transnasional merupakan pergerakan berbagai hal, yang kasat mata maupun tidak, menembus tapal batas negara, dimana sekurang-kurangnya salah satu aktornya tidak mewakili suatu organisasi pemerintah atau antara pemerintah.[15]

Pandangan Koehane dan Nye mengandung dua variabel, yaitu bahwa terdapat pergerakan yang menembus tapal batas negara dan salah satu aktornya bukan merupakan wakil negara atau tidak bertindak atas nama negara. Interaksi transnasional menggambarkan suatu kompleksitas yang relatif rumit, dengan peran negara yang relatif terbatas dalam interaksi tersebut.

---

[15] Walter S. Jones, 1993, *Logika Hubungan Internasional 2*, Jakarta : Gramedia. h. 466.

Memperkuat defenisi-defenisi lainnya bahwa keterlibatan negara atau pemerintah dalam interaksi ini sangat kecil dan terbatas sebaliknya aktor-aktor non-negara memiliki peranan yang besar dalam interaksi ini. Karakteristik atau sifat dasar dari transnasionalisme ini membuat transnasionalisme sebagai suatu interaksi yang sangat kompleks jika dibandingkan dengan interaksi-interaksi internasional lainnya disebabkan begitu banyaknya aktor-aktor yang terlibat. Selain itu, banyaknya kepentingan-kepentingan yang terlibat dalam interaksi ini baik itu individu maupun kelompok memunculkan bentuk-bentuk baru interkasi yang terjadi di dalamnya serta belum memadainya perangkat hukum yang dapat mengaturnya.

Seiring dengan perkembangan teknologi informasi dan komunikasi yang begitu cepat, interaksi transnasional telah menjadi hal yang mudah dan merupakan kebutuhan hampir semua orang. Kebutuhan orang akan informasi dan komunikasi sendiri yang juga mendorong perkembangan teknologi ini. Percepatan perkembangan teknologi informasi dan komunikasi lebih tepat dikatakan sebagai suatu revolusi informasi. Kecepatan tinggi perpindahan informasi dan gagasan dalam bentuk data, gambar, dan suara yang berada dalam jaringan global yang menghubungkan ke semua tempat di dunia telah membuktikan bahwa interaksi transnasional dapat dilakukan dengan sangat cepat dan mudah oleh semua pengguna media ini.

Pada dasarnya teknologi informasi adalah perangkat yang berharga karena dapat memberikan berbagai manfaat baik langsung maupun tidak langsung.

Pengetahuan tentang teknologi informasi ini sangat penting, menurut Abdul kadir dan Terra Ch. Triwahyuni[16], hal ini disebabkan karena :

1. Teknologi informasi itu berada dimana-mana,
2. Teknologi informasi dapat membantu manusia menjadi lebih produktif,
3. Teknologi informasi itu menggairahkan dan dapat memberikan perubahan,
4. Teknologi informasi dapat mempertinggi karir,
5. Teknologi informasi dapat memberikan kesempatan luas kepada manusia di dunia ini.

Sehingga sejak dasawarsa terakhir, perkembangan teknologi informasi telah memperkuat masyarakat kita dalam bidang informasi.

Kemajuan teknologi media informasi bagi sebagaian besar masyarakat internasional dewasa ini merupakan suatu hal penting dalam memudahkan mereka mendapatkan pelayanan tercepat, mudah dan efektif dalam berinterkasi dengan masyarakat internasional di belahan dunia lainnya. Kebutuhan akan kecepatan, keefektifan, dan kenyamanan dalam berinteraksi secara global mendorong kemajuan teknologi informasi yang begitu pesat seperti yang terjadi sekarang ini. Penggunaan teknologi informasi yang berkembang dengan sangat pesat dalam globalisasi ini memungkinkan tidak adanya batasan waktu dan tempat dalam melakukannya.

Rosenau menggambarkan ketekaitan antara kemajuan teknologi dan kemajuan informasi dan komunikasi sebagai berikut :

> *It is technology too, that has so greatly diminished geographic and social distance through the jet-powered airliner, the computer, the orbiting satelite, and the many other innovations that now move*

[16] Abdul Kadir & Terra Ch Triwahyuni, 2003, *Pengenalan Teknologi Informasi*, Yogyakarta : Andi Offset. h. 5

people, ideas, and goods more rapidly and surely across space and time than ever before.

Rosenau menggambarkan peranan teknologi dalam hubungan internasional sebagai berikut :

> *Technology has expanded the capacity to generate and manipulate information and knowledge even more ability to produce material goods, leading to a situation in which the service industries have come to replace the manufacturing industries as the cutting edge of societal life.* [17]

Penjelasan Rosenau di atas menunjukkan bahwa pengaruh teknologi dalam meneruskan informasi mengalami kemajuan yang pesat dibandingkan dengan produksi barang-barang material. Hal ini menjadikan kehidupan sosial masyarakat internasional yang sebelumnya dipengaruhi oleh tingkat produksi dan kepemilikan alat-alat produksi kini beralih kepada penguasaan informasi dan kepemilikan sumber-sumber informasi. Ungkapan bahwa "jika ingin menguasai dunia kuasailah sumber informasi dan media" menjadi ungkapan yang sangat tepat melihat perkembangan berbagai media teknologi informasi yang semakin cepat sekarang ini mampu menjadi suatu kekuatan tersendiri terutama dalam pembentukan budaya global atau *global culture* dan opini publik internasional terhadap masalah internasional.

Dengan kemajuan yang sangat pesat pada perkembangan teknologi informasi maka perpindahan arus informasi menjadi sangat mudah, cepat dan efisien. Masyarakat internasional tidak lagi terbatas pada ruang dan waktu dalam menjalin hubungan baik secara individual maupun kelompok dengan masyarakat lainnya

---

[17] James N Rosenau, *Op Cit.*, h. 445

melewati lintas batas territorial suatu negara. Banyaknya *virtual space*[18] yang bermunculan akibat dari ditemukannya internet yang tidak lain merupakan suatu tempat yang bersifat maya semakin menjadikan kerancuan akan batas-batas teritorial semua negara yang ada di dunia ini. Pembahasan mengenai kemunculan internet, *virtual space*, dan berbagai permasalahannya akan dibahas lebih lanjut pada bab selanjutnya.

Interaksi transnasionalisme dengan menggunakan media teknologi informasi menjadi suatu kajian baru bagi studi hubungan internasional dalam menganalisa efek global yang terjadi dari interaksi yang terjadi di dalamnya. Hal ini terlihat dari penggunaan media teknologi informasi yang dilakukan dapat bersifat individual maupun kelompok atau organisasi *non-governmnet*. Untuk pembahasan berikutnya akan dijelaskan dampak atau pengaruh teknologi informasi.

B. Konsep Kejahatan Transnasional dan *Cyber Crime*

Pada perkembangan kemajuan ilmu pengetahuan dan teknologi dalam kenyataannya tidak hanya menciptakan berbagai kemudahan dan kenikmatan dalam peri kehidupan manusia, namun juga melahirkan berbagai problematika hukum seiring dengan perubahan sistem nilai dalam masyarakat. Salah satu masalah hukum yang ditimbulkan adalah semakin menggejalanya kejahatan-kejahatan yang terjadi di dalam interaksi transnasional dalam berbagai ragam dan bentuk yang biasanya dikenal dengan istilah *transnational crime* atau kejahatan transnasional. Hal itu

[18] *Virtual Space* atau biasa disebut *Cyber Space* : istilah yang dipakai untuk menyebut ruang maya yang terdapat dalam internet atau jaringan.

sangat ditunjang oleh kemajuan ilmu pengetahuan dan teknologi, terutama di bidang transportasi, telekomunikasi, dan komputer.

Istilah transnasionalisme pertama kali muncul di awal abad ke 20 untuk menggambarkan cara pemahaman baru tentang hubungan antar kebudayaan. Ia adalah sebuah gerakan sosial yang tumbuh karena meningkatnya interkonektifitas antar manusia di seluruh permukaan bumi dan semakin memudarnya batas-batas negara. Perkembangan telekomunikasi, khususnya internet, migrasi penduduk dan terutama globalisasi menjadi pendorong perkembangan transnasionalisme ini.

Selain itu, istilah "*transnational crime*" pertama kali digunakan pada konferensi PBB tentang kejahatan dan hukum kriminal (*United Nations Crime and Criminal Justice Branch*) pada tahun 1974 sebagai bahan kajian diskusi di dalam salah satu forumnya. Kemudian pada tahun 1995, PBB memberikan satu konsep tentang kejahatan transnasional sebagai "*offenses whose inception, prevention and or direct effects or indirect effects involved more than one country*" (*United Nations*, 1995).[19]

Kejahatan transnasional berangkat dari pendapat yang dikemukakan oleh Bassiouni menyebutkan bahwa :

> Suatu tindak pidana internasional harus mengandung tiga unsur yakni : unsur internasional, unsur transnasional, dan unsur kebutuhan (*necessity*). Unsur internasional ini meliputi unsur ancaman secara langsung terhadap perdamaian dunia, ancaman secara tidak langsung atas perdamaian dan keamanan di dunia, dan menggoyahkan perasaan kemanusiaan. Unsur transnasional meliputi unsur : tindakan yang

[19] Http://www.YadeSetiawanUjung.com, "Kejahatan Transnasional", diakses pada tanggal 26 Agustus 2009

> memiliki dampak terhadap lebih dari satu negara, tindakan yang melibatkan atau memberikan dampak terhadap warga negara dari lebih satu Negara, dan sarana prasarana serta metode-metode yang dipergunakan melampaui batas teritorial suatu negara. Sedangkan unsur kebutuhan (*necessity*) termasuk ke dalam unsur kebutuhan akan kerjasama antara negara negara untuk melakukan penanggulangan. [20]

Dari pengertian Bassiouni ini dapat dilihat bahwa kejahatan transnasional itu adalah kejahatan yang tidak mengenal batas teritorial suatu negara (*borderless*). Modus operandi, bentuk atau jenisnya, serta letaknya melibatkan beberapa negara dan sistem hukum berbagai negara.

Kejahatan transnasional atau *transnational crime* harus dibedakan dengan kejahatan internasional. PBB memberikan ruang lingkup pada kejahatan transnasional dengan memberikan batasan pada tindak kriminal internasional yang dapat dikategorikan sebagai kejahatan transnasional yaitu kejahatan (dalam hal ini tidak melibatkan suatu pemerintah atau negara) tersebut harus terjadi melintasi batas dari teritorial yurisdiksi hukum suatu negara.

PBB mengidentifikasikan kejahatan transnasional dalam 18 bagian yaitu :

1. *money laundering*
2. *terrorist activities*
3. *theft of art and cultural objects*
4. *theft of intellectual property*
5. *illicit traffic in arms*
6. *sea piracy*
7. *hijacking on land*
8. *insurance fraud*
9. *computer crime*
10. *environmental crime*
11. *trafficking in persons*
12. *trade human body parts*

---

[20] *Ibid.*,

13. *illicit drug trafficking*
14. *fraudulent bankruptcy*
15. *infiltration of legal business*
16. *corruption*
17. *bribery of public officials*
18. *other offences committed by organized criminal groups* (*United Nations*, 1995)[21]

Dari pemaparan tersebut diatas maka dapat disimpulkan bahwa kejahatan transnasional merupakan sutau permasalahan yang menyangkut masalah yurisdiksi hukum yang penyelesaiannya sangat kompleks disebabkan oleh adanya perbedaan yang signifikan pada yurisdiksi hukum setiap negara yang terlibat jika dibandingkan dengan kejahatan transnasional yang dapat diidentifikasi dengan jelas dan penyelesaiannya dapat dilakukan dengan menggunakan hukum internasional. Dari berbagai macam jenis kejahatan transnasional tersebut di atas maka yang akan kita bahas lebih lanjut adalah *computer crime* atau sering juga disebut dengan *cyber crime*.

Berbicara masalah *cyber crime* tidak lepas dari permasalahan keamanan jaringan komputer atau keamanan informasi berbasis internet dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggannya. Untuk mencapai tingkat kehandalan tentunya informasi itu sendiri harus selalau dimutakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya (*cyber crime*) ini muncul seiring

[21] *Loc. Cit.*,

dengan perkembangan teknologi informasi yang begitu cepat. Untuk lebih mendalam ada beberapa pendapat tentang apa yang dimaksud dengan *cyber crime*.

Defenisi *cyber crime* menurut Kepolisian Inggris adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.[22]

Sedangkan menurut Peter, *Cyber crime* adalah :

> *"The easy definition of cyber crime is crimes directed at a computer or a computer system. The nature of cyber crime, however, is far more complex. As we will see later, cyber crime can take the form of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system."* [23]

Sementara itu, Indra Safitri mengemukakan bahwa *cyber crime* atau kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.[24]

Dikdik M Arief Mansyur dan Elisatris Gultom menjelaskan *cyber crime* sebagai berikut :

---

[22] Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, Bandung : PT. Refika Aditama. h. 40

[23] Peter Stephenson, 2000, *Investigating Computer-Related Crime : A Hanbook For Corporate Investigators*, London New York Washington D.C : CRC Press, h. 56

[24] Indra Safitri, "Tindak Pidana di Dunia Cyber". *Insider, Legal Journal From Indonesian Capital & Investmen Market*, http://business.fortunecity.com/buffett/842/art180199_tindakpidana.htm, diakses pada tanggal 20 Agustus 2009

> Upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut.[25]

Berdasarkan definisi tersebut, yang menjadi cakupan dari *cyber crime* menurut Dikdik M Arief Mansyur dan Elisatris Gultom hanyalah terbatas pada kejahatan terhadap perangkat komputer. Sedangkan dalam perkembangannya, *cyber crime* tidak terbatas pada kejahatan terhadap perangkat komputer, tetapi ada kejahatan yang memanfaatkan komputer untuk melakukan kejahatan lain. Seharusnya konsep ini juga termasuk kedalam *cyber crime*. Untuk itu perlu membagi *cyber crime* ke dalam dua garis besar, yaitu kejahatan yang menggunakan teknologi informasi (TI) sebagai fasilitas dan kejahatan yang menjadikan sistem dan fasilitas TI sebagai sasaran.[26]

Pendapat tersebut sejalan dengan dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian *cyber crime*, yaitu *cyber crime* dan *computer related crime*.[27] Dalam *background paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah *cyber crime* dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*.

---

[25] Dikdik M Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law : Aspek Hukum Teknologi Informasi*, Bandung : PT. Refika Aditama. h. 8

[26] Arif Pitoyo, "*Perlunya Penyempurnaan Hukum Pidana Tangani Cybercrime*," http://gerbang.jabar.go.id/gerbang/index.php?index=16&idberita680, diakses pada tanggal 29 Agustus 2009.

[27] Barda Nawawi Arief, 1998, *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*, Bandung : PT Citra Aditya Bakti. h. 24

Kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime*. Lengkapnya sebagai berikut :

1. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed byh 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.*

Pengertian computer dalam *The Proposed West Virginia Computer Crimes Act* adalah

> *"an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typewriter or type-setter, a portable hand-held calculator, or other similar device".*[28]

Dari pengertian kejahatan komputer menurut peraturan perundang-undangan di Virginia dapat dipahami bahwa sesuatu yang berhubungan dengan peralatan pemerosesan data listrik, magnetic, optic, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melalukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau tipe-setter, sebuah kalkulator tangan atau peralatan serupa lainnya.

---

[28] Abdul Wahid dan Mohammad Labib, *Op, Cit.*, h. 41

Di lihat dari beberapa definisi di atas, tampak bahwa belum ada kesepakatan mengenai definisi tentang *cyber crime* atau kejahatan dunia *cyber*. Menurut Muladi, sampai saat ini belum ada definisi yang seragam tentang *cyber crime* baik nasional maupun global. Kebanyakan masih menggunakan *soft law* berbentuk *code of conduct* seperti Jepang dan Singapura.[29]

C. Kerjasama Keamanan Internasional

Kerjasama merupakan salah satu kegiatan dalam dan luar negeri yang dapat dilakukan oleh suatu negara demi tercapainya tujuan suatu negara tersebut. Dalam hubungan internasional, kerjasama bisa dilakukan di dalam segala aspek kehidupan, diantaranya dalam bidang ekonomi, politik, sosial, budaya, pendidikan, keamanan dan aspek-aspek lainnya. Dengan adanya ketergantungan ini, maka secara otomatis akan menimbulkan suatu hubungan timbal balik antara negara kerjasama dalam bidang tertentu, yang nantinya akan saling menguntungkan masing-masing negara.

Dalam melakukan kerjasama internasional, paling tidak ada dua hal yang penting untuk dilakukan. Pertama, adanya keharusan untuk menghargai kepentingan nasional masing-masing anggota yang terlibat. Tanpa adanya penghargaan, tidak akan mungkin tercapai suatu kerjasama yang diharapkan. Kedua, adanya keputusan bersama atau komitmen dalam mengatasi masalah yang dihadapi. Untuk mencapai komitmen maka diperlukan komunikasi dan konsultasi yang bahkan terkadang lebih penting daripada komitmen. Dengan kata lain, frekuensi komunikasi dan konsultasi harus lebih tinggi dari pada komitmen.

---

[29] http://www.suaramerdeka.com/harian/0207/24/nas13.htm. diakses pada tanggal 25 Agustus 2009

Konsep kerjasama keamanan sering diartikan sama dengan aliansi keamanan. Meskipun ruang lingkup konsep kerjasama keamanan lebih luas dan kerjasama keamanan belum tentu berupa aliansi. Aliansi keamaman lebih terfokus pada kerjasama keamanan melalui sebuah perjanjian dimana sangat berpengaruh pada kebijakan luar negeri negara yang menyangkut pertahanan keamanan negara. Konsep aliansi sangat berkaitan erat dengan konsep "*balance of power*".

Ketika suatu aliansi berada pada tampuk kekuasaan, maka negara-negara netral biasanya bergabung dengan aliansi lemah untuh mencegah aliansi lain dalam memperoleh hegemoni. Hal tersebut sering menjadikan konsep kerjasama keamanan diartikan dengan kerjasama kebijakan luar negeri yang menyangkut pertahanan dan keamanan yang mana instrument yang sering digunakan adalah militer dan persenjataan. Sedangkan konsep kerjasama keamanan dengan ruang lingkup lebih luas mencakup kerjasama keamanan yang didasari oleh kepentingan pertahanan dan keamanan serta kerjasama yang didasari oleh kepentingan penegakan hukum dan ekonomi.

Dikarenakan faktor interdependensi, maka negara akan selalu terkena pengaruh oleh semua tindakan yang dilakukan oleh aktor-aktor hubungan internasional lainnya dan kerjasama adalah salah satu bentuk respon terhadap dinamika yang ditimbulkan oleh aktor-aktor hubungan internasional tersebut. Kerjasama internasional dalam perspektif Neo-realisme dimungkinkan terjadi dalam pola hubungan antar negara atau aktor internasional. Kerja sama dimungkinkan dikarenakan negara atau aktor internasional dalam sistem internasional berusaha

untuk meningkatkan kapabilitas mereka. Neo-realis memastikan bahwa kerjasama internasional tidak dapat diwujudkan kecuali negara-negara membuatnya terjadi. Neo-realis juga beranggapan, walau mungkin terwujud, kerjasama akan sulit untuk dipertahankan dan tergantung dari power negara itu sendiri.[30]

Holsti mengklasifikasikan kerjasama kedalam bidang-bidang kerjasama yang dilakukan, yaitu :[31]

a. Kerjasama universal (global) yang melibatkan semua bangsa di dunia yang tergabung dalam suatu cita-cita bersama dengan kata lain merupakan integrasi internasional.
b. Kerjasama regional yang dilakukan oleh negara-negara yang berdekatan secara geografis, memiliki politik dan budaya yang relatif sama tapi struktur produktivitas dan kemampuan yang berbeda mendorong mereka untuk bekerja sama.
c. Kerjasama fungsional untuk mendukung fungsi dan tujuan bersama. Kerja sama fungsional bertolak belakang dari cara pikir yang pragmatis yang mengisyaratkan kemampuan tertentu pada masing-masing mitra kerja samanya.
d. Kerjasama ideologis yang dilakukan karena adanya kesamaan pandangan yang berkaitan dengan ideologi dan hal ini mempengaruhi perilaku mereka dalam kerja samanya.

Kerjasama internasional dikelompokkan menurut isinya, adalah :

a. Segi politis, seperti Pakta Pertahanan yang dibentuk ketika Perang Dingin untuk saling membendung ideologi lawan. Contoh: NATO, ANZUS, SEATO, Pakta Warsawa.
b. Segi ekonomi, seperti bantuan ekonomi dan bantuan keuangan. Contoh: IMF, CGI, IBRD, World Bank.
c. Segi hukum, seperti status kewarganegaraan (Indonesia-RRC), ekstradisi tersangka kejahatan.
d. Segi kesehatan, seperti masalah karantina, penanggulangan wabah yang melintasi antarnegara (AIDS, SARS dll).
e. Segi teritori, seperti menentukan batas laut dan daratan negara satu dengan negara lain yang berbatasan langsung.

---

[30] Ken Booth and Steve Smith, 1995, *International Relations Theory Today*. Penn State. h. 4-8
[31] Kj Holsti, *Op. Cit.*, h. 589

Kerjasama bisa timbul dari suatu komitmen terhadap kesejahteraan bersama atau sebagai usaha untuk memenuhi kepentingannya. Kunci dari perilaku kerjasama ada pada sejauh mana setiap pihak yang bekerjasama percaya bahwa yang lainnya akan mematuhi kaidah-kaidah yang telah ditetapkan dalam kerja sama. Isu utama dari konsep kerjasama adalah pemenuhan kebutuhan pribadi, dimana hasil yang menguntungkan kedua belah pihak akan diperoleh melalui kerjasama daripada berusaha memenuhi kepentingannya dengan berusaha sendiri.[32]

Negara bukan peserta kerjasama yang pada hakikatnya tidak memiliki hak dan kewajiban untuk patuh. Akan tetapi, bila perjanjian itu bersifat multilateral (PBB) atau objeknya dinilai penting, maka negara lain yang diluar kerjasama juga dapat terikat, apabila negara tersebut menyatakan diri terikat terhadap perjanjian yang telah dibuat dan bersedia untuk mematuhi dan negara tersebut dikehendaki oleh para peserta.[33] Setiap negara pasti mempunyai kelebihan dan kekurangannya. Oleh sebab itu, dengan adanya kerjasama antar negara satu sama lain dapat saling menyalurkan kelebihannya dan menutupi kekurangannya. Dengan demikian, pembangunan di negara kita maupun di negara lain akan berjalan dengan lancar sehingga negara kita dapat membangun, serta menciptakan keadilan dan kesejahteraan sosial bagi seluruh rakyatnya dan menciptakan saling pengertian antar bangsa dalam membina dan menegakkan perdamaian dunia.

---

[32] James E Dougherty dan Robert L Pfaltzgraff, 1997. *Contending Theories of International Relations : A Comprehensive Survey*. New Yorl : Longman. h. 418-419

[33] *Ibid.*, hl 420

BAB III

GAMBARAN UMUM *CYBER CRIME* DAN KERJASAMA INTERNASIONAL

A. *Cyber Crime* (Kejahatan Dunia Maya)

Perkembangan teknologi informasi, telekomunikasi serta transaksi elektronik, selain telah memberikan sumbangan bagi peningkatan kesejahteraan, kemajuan dan peradaban hidup manusia, juga menjadi sarana yang lebih efektif bagi sebagian orang atau kelompok orang dalam memanfaatkannya untuk melawan hukum atau melakukan kejahatan, sehingga menghasilkan tindakan yang merugikan masyarakat. Dengan menggunakan bantuan teknologi informasi, telekomunikasi serta transaksi elektronik, kejahatan menjadi semakin mudah, cepat, leluasa dan semakin instan untuk dilakukan. Salah satu kejahatan yang paling marak dalam ruang lingkup teknologi informasi yaitu *cyber crime*. *Cyber crime* adalah kejahatan yang memanfaatkan teknologi informasi dengan segala macam penggunaan jaringan komputer untuk tujuan kriminal dan atau kriminal berteknologi tinggi dengan menggunakan kemudahan teknologi digital. Namun, *cyber crime* pada dasarnya merupakan kejahatan lama (konvensional) tetapi menggunakan teknologi baru.

1. Perkembangan *Cyber Crime*

Cyber crime dalam perkembangannya dapat terlihat pada pesatnya perkembangan globalisasi di bidang teknologi informasi saat ini yang merupakan dampak dari semakin kompleksnya kebutuhan manusia akan informasi itu sendiri. Dekatnya hubungan antara informasi dan teknologi jaringan komunikasi telah

menghasilkan dunia maya yang amat luas yang biasa disebut dengan teknologi *cyber space*. Teknologi ini berisikan kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan komputer yang disebut jaringan internet. Sebagai media penyedia informasi internet juga merupakan sarana kegiatan komunitas komersial terbesar dan terpesat pertumbuhannya. Sistem jaringan memungkinkan setiap orang dapat mengetahui dan mengirimkan informasi secara cepat dan menghilangkan batas-batas teritorial suatu wilayah negara.

Dalam era globalisasi perkembangan terjadi sangat cepat seiring dengan peningkatan teknologi informasi, salah satunya adalah internet, yang telah menjadi sarana informasi yang sangat populer dewasa ini. Hal tersebut menghilangkan batas wilayah antar negara yang menjadikan dunia ini begitu sempit dan membuat penyebaran informasi serta komunikasi menjadi mudah. Kecanggihan dan keakuratan komputer dalam mengolah dan memanipulasi data, khususnya internet juga dapat menimbulkan kejahatan yang didalamnya memiliki media komunikasi publik baru untuk bekerja. Dunia internet merupakan media yang nyaman dan menjadi tempat yang spesial untuk melakukan kejahatan. Mulai dari penipuan sederhana sampai yang sangat merugikan, ancaman terhadap seseorang atau kelompok, penjualan barang-barang ilegal, sampai tindakan terorisme yang bisa dilakukan dengan menggunakan komputer dan Internet.

Globalisasi aktivitas kriminal dan anonimitas yang memungkinkan para penjahat melintas batas elektronik merupakan masalah nyata dengan potensi mempengaruhi setiap negara, hukum dan warga negara. Hal ini dikarenakan sarana-

sarana yang digunakan untuk melakukan aktivitas ini bukan tergolong peralatan yang murah. Meskipun pada dasarnya interaksi internet bersifat bebas dan pribadi, namun kebebasan *cyber* dalam aktivitas internet itu haruslah dilakukan sedemikian rupa sehingga tidak merugikan kepentingan umum atau konsumen, melanggar hak pribadi orang lain, mengganggu keamanan nasional, mengancam integritas bangsa serta melanggar nilai dan norma kesusilaan dan moralitas. Statistik terakhir memperlihatkan bahwa penetrasi internet pada tahun 2008 telah mencapai kurang lebih 21% dari total 6,676 milyar penduduk bumi. Artinya adalah bahwa satu dari lima individu di dunia ini adalah pengguna internet.

Gambar 1. Estimasi Profil Pengguna Internet di Lima Benua Tahun 2008

WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2008 Est.)	Population % of World	Internet Usage, Latest Data	% Population (Penetration)	Usage % of World	Usage Growth 2000-2008
Africa	955,206,348	14.3 %	51,022,400	5.3 %	3.6 %	1030.2 %
Asia	3,776,181,949	56.6 %	529,701,704	14.0 %	37.6 %	363.4 %
Europe	800,401,065	12.0 %	382,005,271	47.7 %	27.1 %	263.5 %
Middle East	197,090,443	3.0 %	41,939,200	21.3 %	3.0 %	1176.8 %
North America	337,167,248	5.1 %	246,402,574	73.1 %	17.5 %	127.9 %
Latin America/Caribbean	576,091,673	8.6 %	137,300,309	23.8 %	9.8 %	659.9 %
Oceania / Australia	33,981,562	0.5 %	19,353,452	57.0 %	1.4 %	154.0 %
WORLD TOTAL	6,676,120,288	100.0 %	1,407,724,920	21.1 %	100.0 %	290.0 %

Sumber : *Cyber* 6. Enam Aspek Menjaga dan Melindungi Dunia Maya. Oleh Prof. Richardus Eko Indrajit

Internet selain memberi manfaat ternyata membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak terpikirkan akan terjadi. Kejahatan yang lahir sebagai

dampak negatif dari perkembangan aplikasi internet ini sering disebut *cyber crime* atau kejahatan dunia maya. Kejahatan di dunia maya merupakan salah satu jenis kejahatan atau tindak pidana yang dilakukan dengan memanfaatkan teknologi informasi yakni komputer. Ada beberapa jenis kejahatan *cyber crime* yang cukup menonjol seperti pengedaran program komputer tanpa ijin, pencemaran nama baik lewat Internet, *carding* atau penipuan pembelian barang dengan kartu kredit palsu serta serangan virus atau worm. Hal itu terjadi pula untuk data dan informasi yang dikerjakan secara elektronik.

Para pelaku *cyber crime* melakukan tindakan kejahatannya dengan berbagai modus operandi untuk mewujudkan tindakannya yang memanfaatkan sarana dan prasarana teknologi informasi dan komunikasi serta dapat dilakukan oleh siapa saja tanpa mengenal batas wilayah. Ruang *cyber* merupakan suatu tempat yang hanya dibatasi oleh screen and passwords. Selain tidak mengenal batas-batas wilayah, kejahatan tersebut juga memiliki karakteristik yang khusus, sehingga dalam pengaturan dan penegakkan hukumnya pun tidak dapat menggunakan cara-cara maupun hukum tradisional dan harus diatur di dalam hukum tersendiri.

2. Kategori *Cyber Crime*

Cyber crime sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik tersendiri yang berbeda dengan kedua model di atas. Karakteristik unik dari kejahatan di dunia maya tersebut antara lain menyangkut lima hal. Diantaranya mencakup ruang lingkup kejahatan,

sifat kejahatan, pelaku kejahatan, modus kejahatan, dan jenis kerugian yang ditimbulkan.[34]

Dengan pembagian kategori *cyber crime* tersebut, terdapat beberapa jenis *cyber crime* yang dikenal saat ini. Dikdik M. Areif Mansur dan Elisatris Gultom menjelaskan jenis kejahatan yang termasuk dalam kategori *cyber crime*, diantaranya sebagai berikut :[35]

1. *Cyber-terorisme.*
2. *Cyber-pornography.* Penyebaran *obscene* materials termasuk *pornography, indencent exposure*, dan *child pornograpy.*
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.

Berdasarkan jenis aktifitas yang dilakukannya, *cyber crime* dapat digolongkan menjadi beberapa jenis sebagai berikut :[36]

a. *Unauthorized Access*, merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.
b. *Illegal Contents*, merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau

[34] http://cybercrime.wordpress.com/, diakses pada tanggal 25 Agustus 2009
[35] Dikdik M Arief Mansur dan Elisatris Gultom, *Op. Cit.*, h. 26
[36] http://www.duniamaya.org/index.php/security/kejahatan-dunia-maya-cybercrime/, diakses pada tanggal 25 Agustus 2009

menggangu ketertiban umum, contohnya adalah penyebaran pornografi.

c. *Penyebaran virus secara sengaja*, penyebaran virus pada umumnya dilakukan dengan menggunakan e-mail. Sering kali orang yang sistem e-mailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui e-mailnya.
d. *Data Forgery*, kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis *web database*.
e. *Cyber Espionage, Sabotage, and Extortion*, *Cyber Espionage* merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
f. *Cyberstalking*, kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.
g. *Carding*, *carding* merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.
h. *Hacking dan Cracker*, istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang *cracker* ini sebenarnya adalah *hacker* yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan *account* milik orang lain, pembajakan situs web, *probing*, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (*Denial Of Service*). *Dos attack* merupakan serangan yang bertujuan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan.
i. *Cybersquatting and Typosquatting*, *Cybersquatting* merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama

perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

j. *Hijacking, hijacking* merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak).
k. *Cyber Terorism*, suatu tindakan *cyber crime* termasuk *cyber terorism* jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer. Beberapa contoh kasus *cyber terorism* sebagai berikut :
    - Ramzi Yousef, dalang penyerangan pertama ke gedung WTC, diketahui menyimpan detail serangan dalam file yang di enkripsi di laptopnya.
    - Osama Bin Laden diketahui menggunakan steganography untuk komunikasi jaringannya.
    - Suatu website yang dinamai *Club Hacker* Muslim diketahui menuliskan daftar tip untuk melakukan hacking ke Pentagon.
    - Seorang *hacker* yang menyebut dirinya sebagai Doktor Nuker diketahui telah kurang lebih lima tahun melakukan defacing atau mengubah isi halaman web dengan propaganda anti-American, anti-Israel dan pro-Bin Laden.

Secara garis besar, ada beberapa tipe *cyber crime*, seperti dikemukakan Philip Renata yaitu :[37]

a. *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi komputer.
b. *Hacking*, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.
c. *The Trojan Horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi pribadi atau orang lain.
d. *Data Leakage*, yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa berupa rahasia negara, perusahaan, data

[37] *Loc. Cit.*

yang dipercayakan kepada seseorang dan data dalam situasi tertentu.

e. *Data Diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah *input* data atau *output* data.
f. *To frustate data communication* atau penyia-nyiaan data komputer.
g. *Software piracy* yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HAKI.

Dari ketujuh tipe c*yber crime* tersebut, nampak bahwa inti *cyber crime* adalah penyerangan di *content, computer system* dan *communication system* milik orang lain atau umum di dalam *cyber space*.[38]

Sementara itu P.N Grabosky dan Russell G. Smith menjabarkan bentuk-bentuk *cyber crime* sebagai berikut :[39]

a. *Illegal interception of telecommunications*
b. *Electronic vandalism and terrorism*
c. *Stealing telecommunications services*
d. *Telecommunications piracy*
e. *Pornogrhapy and other offensive content*
f. *Telemarketing fraud*
g. *Electronic funds transfer crime*
h. *Electronic money laundering*
i. *Telecommunications in furtherance of criminal conspiracies*

Pengkategorian yang diberikan oleh Grabosky dan Smith di atas mempunyai cakupan yang luas dengan menambahkan kejahatan digital atau *electronic crime* seperti penyadapan dan pembajakan saluran telekomunikasi telepon sebagai bagian dari *cyber crime*. Dalam hal ini, *cyber crime* diasosiasikan dengan betuk-bentuk kejahatan yang bersifat *hi-tech crime* yaitu suatu tindakan kriminal yang

---

[38] Edmon Makarim, 2005, *Pengantar Hukum Telematika : Suatu Kompilasi Kajian.* Jakarta : PT RajaGrafindo Persada. h. 12

[39] P.N Grabosky dan Russell G. Smith, 1998, *Crime in the Digital Age : Controlling Telecommunications and Cyberspaces Illegalities*, New Brunswick : Transaction Publishers. h. 144

memanfaatkan kemajuan teknologi sebagai alat atau media dalam melakukan aksinya. Sedangkan menurut Eoghan Casey "*Cyber crime is used throughout this text to refer to any crime that involves computer and networks, including crimes that do not rely heavily on computer*".[40] Ia mengkategorikan *cyber crime* dalam 4 kategori yaitu :

a. *A computer can be the object of crime.*
b. *A computer can be the subject of crime.*
c. *The computer can be used as the tool for conducting or planning a crime.*
d. *The ymbol of the computer it self can be used to intimidate or deceive.*[41]

Klasifikasi yang diberikan oleh Casey tersebut memberikan lingkup yang lebih luas pada *cyber crime* yaitu dengan mencakup kejahatan yang tidak secara langsung menggunakan komputer sebagai alat utama, seperti contoh pada kategori ketiga yang menjadikan tindakan seperti perencanaan kejahatan yang dilakukan menggunakan komputer sebagai bagian dari *cyber crime*. Sejalan dengan pembagian yang diberikan oleh Casey tersebut *cyber crime* secara teknis dapat dibedakan menjadi *offline crime, semi online crime*, dan *online crime*. Dalam pengertian komputer yang tidak terhubung ke dalam jaringan atau internet dapat dijadikan sebagai alat maupun objek dari tindakan *cyber crime*, sebagai contoh komputer yang digunakan untuk pembuatan virus yang dapat menyebarkan virus tersebut melalui

---

[40] Casey Eoghan, 2001, *Digital Evidence and Compute Crime*, London : A Harcourt Science and Technology Company. h. 16
[41] *Loc. Cit.*

media *removable devices* seperti *flash disk, memory card*, maupun *cd-room* dan *dvd-room* yang semakin banyak digunakan akhir-akhir ini.

Fenomena *cyber crime* memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cyber crime* dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global *internet*, semua negara yang melakukan kegiatan *internet* hampir pasti akan terkena imbas perkembangan *cyber crime* ini. Melihat besarnya dampak yang ditimbulkan dari *cyber crime* tersebut maka salah satu solusi terbaik yang harus dilakukan adalah dengan mengadakan kerjasama internasional dalam membangun sekuritas jaringan teknologi informasi yang dilakukan secara bersama dengan semua negara yang ada di dunia.

3. *Cyber Terrorism*

Berdasarkan berbagai jenis *cyber crime* tersebut, terlihat variasi dari *cyber crime*, dimana beberapa kejahatan bertujuan untuk menyerang sistem komputer (*hacking*) dan kejahatan lain hanya memanfaatkan infrastruktur dan sistem komputer (*cyber pornography).* Dari ragam jenis *cyber crime* tersebut, yang menjadi fokus dalam pembahasan ini adalah *cyber terrorism.* Mengingat *cyber terrorism* ini adalah kejahatan yang bersifat melintasi batas negara dan termasuk kejahatan transnasional.

Dalam beberapa kasus, penguasaan terhadap teknologi sering kali disalahgunakan untuk melakukan suatu kejahatan. Diantara ragam kejahatan menggunakan teknologi, terdapat didalamnya suatu bentuk kejahatan terorisme baru, yaitu *cyber terrorism*. Akar perkembangan dari *cyber terrorism* dapat ditelusuri sejak

awal 1990, ketika pertumbuhan Internet semakin pesat dan kemunculan komunitas informasi. Di Amerika serikat sejak saat itu diadakan kajian mengenai potensi resiko yang akan dihadapi Amerika Serikat atas ketergantungannya yang begitu erat dengan jaringan (*networks*) dan teknologi tinggi.[42] Dikhawatirkan, karena ketergantungan Amerika Serikat yang begitu tinggi terhadap jaringan dan teknologi suatu saat nanti Amerika akan menghadapi apa yang disebut "*Electronic Pearl Harbor*".[43]

Faktor psikologis, politik, dan ekonomi merupakan kombinasi yang menjadikan peningkatan ketakutan Amerika terhadap isu terkait *cyber terrorism*. Sehingga pada tahun 1999, Presiden Clinton sampai mengajukan proposal anggaran dana untuk menangani aksi *cyber terrorisme* sebesar $2.8 miliar. Dana tersebut juga diperuntukan bagi penanganan keamanan nasional dari ancaman bahaya internet.[44]

Ketakutan tersebut cukup beralasan, karena telah terjadi beberapa insiden yang dikategorikan sebagai *cyber terrorism*, antara lain pada April dan Maret 2002, di Amerika Serikat, tepatnya negara bagian California, terjadi kehilangan pasokan listrik secara total yang disebabkan oleh ulah *cracker* dari Cina yang menyusup kedalam jaringan *power generator* di wilayah tersebut.[45]

Contoh lainnya adalah aksi 40 *cracker* dari 23 negara bergabung dalam perang *cyber* konflik Israel-Palestina sepanjang bulan Oktober 2000 sampai Januari 2001.

---

[42] Gabriel Weimann, "*Cyberterrorism: How Real Is the Threat?*," *USIP Special Report No. 119* (December 2004), http://www.usip.org/pubs/specialreports/sr119.html, diakses pada tanggal 29 Agustus 2009

[43] *Ibid.*,

[44] Electronic Civil Defence, http://ntrg.cs.tcd.ie/undergrad/4ba2.02/infowar/ecd.html, diakses pada tanggal 29 Agustus 2009

[45] Wikipedia, http://en.wikipedia.org/wiki/Cyber-terrorism, diakses pada tanggal 29 Agustus 2009

Kelompok yang menamakan dirinya UNITY dan memiliki hubungan dengan organisasi Hezbollah merencanakan akan menyerang situs resmi pemerintah Israel, sistem keuangan dan perbankan, ISPs Israel dan menyerang situs *e-commerce* kaum zionis Israel.[46] Motif dilakukannya *cyberterrorism* menurut Zhang ada lima sebab, yaitu :[47]

1. *Psychological Warfare*. Menurut Zhang, "*The study of the modern terrorism also reveals one of the most important characteristics of the terrorism is to raise fear.*" Motif ini tidak berbeda dengan motif terorisme konvensional, dimana sasaran utama terorisme adalah menimbulkan rasa ketakutan dalam masyarakt.
2. Propaganda. Melalui *cyber terrorism*, kelompok teroris dapat melakukan propaganda tanpa banyak hambatan seperti sensor informasi, karena sifat Internet yang terbuka, upaya ini jauh lebih efektif.
3. *Fundraising*. Melalui *cyber terrorism*, khususnya tindakan penyadapan dan pengambilalihan harta pihak lain untuk kepentingan organisasi teroris telah menjadi motif utama dari *cyber terrorism*. Kelompok teroris juga dapat menambah keuangannya melalui penjualan CD dan buku tentang "perjuangan" mereka.
4. *Communication*. Motif selanjutanya dari *cyber terrorism* adalah komunikasi. Kelompok teroris telah secara aktif memanfaatkan Internet sebagai media komunikasi yang efektif dan jauh lebih aman dibandingkan komunikasi konvensional.
5. *Information Gathering*. Kelompok teroris memiliki kepentingan terhadap pengumpulan informasi untuk keperluan teror, seperti informasi mengenai sasaran teror, informasi kekuatan pihak musuh, dan informasi lain yang dapat menunjang kinerja kelompok teroris tersebut seperti informasi rahasia (*intelegent information*) terkait persenjataan, dan lainnya. Atas dasar motif *information gathering*lah *cyber terrorism* dilakukan.

---

[46] Mansur, *Op. Cit.*, h. 54.
[47] Zhang, http://www.slais.ubc.ca/courses/libr500/04-05-wt1/www/X_Zhang/5ways.htm , **diakses pada tanggal 30 Agustus 2009.**

Pergeseran wilayah terorisme konvensional ke *cyber terrorisme* disebabkan beberapa faktor. Weimann dalam tulisannya www.terror.net : *How Modern Terrorism Uses the Internet* menuturkan delapan alasan mengapa terjadi pergeseran wilayah aktifitas terorisme dari konvensional ke *cyber terrorisme* yaitu sebagai berikut :[48]

1. Kemudahan untuk mengakses. *Cyber terrorism* dapat dilakukan secara remote. Artinya tindakan *cyber terrorism* dapat dilakukan dimana saja melalui pengontrolan jarak jauh.
2. Sedikitnya peraturan, penyensoran, dan segala bentuk kontrol dari pemerintah.
3. Potensi penyebaran informasi yang mengglobal.
4. Anonimitas dalam berkomunikasi. Hal ini merupakan hal yang biasa dalam dunia Internet. Kebanyakan orang berinteraksi di Internet menggunakan nama palsu atau biasa disebut *nickname*.
5. Arus informasi yang cepat.
6. Biaya yang rendah untuk mengembangkan dan merawat website, selain itu dalam melaksanakan *cyber terrorism* yang diperlukan umumnya hanya perangkat komputer yang tersambung ke jaringan Internet.
7. Lingkungan multimedia yang mempermudah penyampaian maksud dan tujuan teror.
8. Kemampuan yang lebih baik dari media massa yang tradisional dalam menyajikan informasi.

Untuk mendalami apa dan bagaimana *cyber terrorism*, maka terlebih dahulu diberikan definisi terhadap kata tersebut. Beberapa lembaga dan ahli memberikan definisi terkait *cyber terrorism*. Definisi pertama didapat dari *Black's Law Dictionary*, yang menjelaskan sebagai berikut :

> *Cyber terrorism. Terrorism committed by using a computer to make unlawful attacks and threats of attack againts computer, networks, and electronically stored information, and actually causing the target to fear or experience harm.*[49]

---

[48] Gabriel Weimann, www.terror.net : *How Modern Terrorism Uses the Internet*, http://www.usip.org/pubs/specialreports/sr116.pdf, diakses pada tanggal 30 Agustus 2009.

[49] Bryan A Graner, 2004, *Black's Law Dictionary Eighth Edition*, West Thomson : St. Paul. h. 5.

Secara bebas dapat diartikan, terorisme yang dilakukan dengan menggunakan komputer untuk melakukan penyerangan terhadap komputer, jaringan komputer, dan data elektronik sehingga menyebabkan rasa takut pada korban. Dari definisi ini terlihat unsur utama dari *cyber terrorism*, yaitu :[50]

a. Penggunaan computer,
b. Tujuannya untuk melakukan penyerangan, serangan tersebut ditujukan kepada sistem komputer dan data, dan
c. Adanya akibat rasa takut pada korban.

Definisi selanjutnya dikeluarkan oleh Federal Bureau of Investigation (FBI) yang menyatakan sebagai berikut ;

> *Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents.*[51]

Secara bebas dapat diterjemahkan menjadi, *cyber terrorism* adalah serangan yang telah direncanakan dengan motif politk terhadap informasi, sistem komputer, dan data yang mengakibatkan kekerasan terhadap rakyat sipil dan dilakukan oleh sub-nasional grup atau kelompok rahasia. Definisi berikutnya diberikan oleh Dorothy Denning, yaitu:

> *Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.*[52]

---

[50] *Ibid.*, h. 6.
[51] Federal Bureau of Investigation (FBI), *citation* Adam Savino, *CyberTerrorisme*, http://www.cybercrimes.net/Terrorism/ct.html, diakses pada tanggal 28 Agustus 2009.
[52] Dorothy Denning, *citation from* Weimann, *op. cit.*

Terjemahan bebasnya adalah, *cyberterrorsim* adalah konvergensi dari *cyber space* dan terorisme. Pengertian tersebut merujuk pada perbuatan melawan hukum dengan cara menyerang dan mengancam melakukan serangan terhadap komputer, jaringan dan informasi yang tersimpan didalamnya untuk tujuan mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik atau sosial. Lebih lanjut, Denning menambahkan, agar dapat dikualifikasikan sebagai *cyberterrorism*, tindakan tersebut juga harus menyebabkan kekerasan terhadap manusia atau kerusakan terhadap benda, atau paling tidak menimbulkan ancaman ketakutan.

Selanjutnya, James A. Lewis memberikan definisi *cyberterrorism* sebagai berikut ;

> *The use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a go vernment or civilian population.*[53]

Definisi yang diberikan James A. Lewis ini hampir sama dengan dua definisi sebelumnya, yaitu penekanan terhadap penggunaan komputer untuk melakukan terorisme dimana target serangannya umumnya adalah sistem komputer juga. Dalam tulisannya yang lain, *The Internet and Terrorism*, Lewis menyatakan sebagai berikut ;

> *The Internet enables global terrorism in several ways. It is an organizational tool, and provides a basis for planning, command, control, communication among diffuse groups with little hierarchy or infrastructure. It is a tool for intelligence gathering, providing access to a broad range of material on potential targets, from simple maps to aerial photographs. One of its most valuable uses is for propaganda,*

[53] James A. Lewis (a), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *Center of Strategic & International Studies* (December 2002): 1.

to relay the messages, images and ideas that motivate the terrorist groups.
Terrorist groups can use websites, email and chatrooms for fundraising by soliciting donations from supporters and by engaging in cybercrime (chiefly fraud or the theft of financial data, such as credit card numbers).[54]

Berdasarkan pernyataan tersebut, kita ketahui kemungkinan atau bentuk lain dari *cyberterrorism*, yaitu pemanfaatan teknologi informasi yang dalam hal ini internet sebagai perangkat organisasi yang berfungsi sebagai alat untuk menyusun rencana, memberikan komando, berkomunikasi antara anggota kelompok. Selain itu, basis teknologi informasi menjadi bagian penting dari terorisme yaitu sebagai media propaganda kegiatan terorisme.

Penggunan basis teknologi informasi sebagai media terorisme telah menunjukan bentuk dan karakter lain dari *cyberterrorism*. Dengan demikian secara garis besar, *Cyberterrorism* dapat dibagi menjadi dua bentuk atau karakteristik, yaitu sebagai berikut : [55]

1. *Cyberterrorism* yang memiliki karkateristik sebagai tindakan teror terhadap sistem komputer, jaringan, dan/atau basis data dan informasi yang tersimpan didalam komputer.
2. *Cyberterrorism* berkarakter untuk pemanfaatan Internet untuk keperluan organisasi dan juga berfungsi sebagai media teror kepada pemerintah dan masyarakat.

4. Kasus *Cyber Crime*

Kebutuhan dan penggunaan akan teknologi formasi yang diaplikasikan dengan internet dalam segala bidang seperti *e-banking, e-commerce, e-government, e-*

[54] James A. Lewis (b), "Internet and Terrorism," *Center of Strategic & International Studies* (April 2005): 1.
[55] *Ibid.*,

education dan banyak lagi telah menjadi sesuatu yang lumrah. Bahkan apabila masyarakat terutama yang hidup di kota besar tidak tersentuh dengan persoalan teknologi informasi yang dapat dipandang terbelakang. Internet telah menciptakan dunia baru yang dinamakan *cyber space* yaitu sebuah dunia komunikasi berbasis computer yang menawarkan realitas yang baru berbentuk *virtual* (tidak langsung dan tidak nyata).

Perkembangan internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif kita semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi ini, misalnya kita dapat melakukan transaksi perbankan kapan saja dengan *e-banking*, *e-commerce* juga membuat kita mudah melakukan pembelian maupun penjualan suatu barang tanpa mengenal tempat. Mencari referensi atau informasi mengenai ilmu pengetahuan juga bukan hal yang sulit dengan adanya *e-library* dan banyak lagi kemudahan yang didapatkan dengan perkembangan internet. Di sisi lain, tidak dapat dipungkiri bahwa teknologi internet membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat dilakukan dengan menggunakan media komputer secara *online* dengan risiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun Negara disamping menimbulkan kejahatan-kejahatan baru.

Kemajuan teknologi telah membawa perubahan dan pergeseran yang cepat dalam suatu kehidupan tanpa batas. Pemanfaatan teknologi tersebut telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi dapat disajikan melalui hubungan jarak jauh dan mereka yang ingin mengadakan transaksi tidak harus bertemu muka, akan tetapi cukup melalui peralatan komputer dan telekomunikasi. Perkembangan teknologi informasi juga membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial dan telah membalikkan segalanya yang jauh jadi dekat yang khayal jadi nyata. Namun dibalik kemajuan itu, juga telah melahirkan keresahan-keresahan baru dengan munculnya kejahatan yang canggih dalam bentuk c*yber crime.*

Dalam konteks *cyber crime* ini erat hubungannya dengan teknologi, khususnya teknologi komputer dan telekomunikasi sehingga pencegahan *cyber crime* dapat digunakan melalui saluran teknologi atau disebut juga *techno-prevention.* Langkah ini sesuai dengan apa yang telah diungkapkan oleh *International Information Industri Congress* (IIIC) sebagai berikut ;

> *The IIIC recognizes that government action and internasional treaties to harmonize laws and coordinate legal procedures are keying the fight cyber crime, but warns that these should not be relied upon as the only instrument. Cyber crime is enabled by technology and requires as healty reliance on technology for its solution.*[56]

Pendekatan teknologi ini merupakan subsistem dalam sebuah sistem yang lebih besar, yaitu pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan atau merupakan kebudayaan itu sendiri. Pendekatan budaya atau cultural

[56] Barda Nawawi Arief, *Op. Cit.*, h. 5.

ini perlu dilakukan untuk membangun atau membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan atau mengajarkan etika penggunaan komputer melalui media pendidikan. Pentingnya pendekatan budaya ini, khususnya dalam upaya mengembangkan kode etik dan perilaku (*code of behavior and ethics*) terungkap juga dalam pernyataan IIIC sebagai berikut ;

> *IIIC members are also committed to participate in the development of code behaviour and ethics around computer and Internet use, and in campaigns for the need for ethical and responsible online behaviour. Given the international reach of Internet crime, computer and Internet users around the world must be made aware of the need for high standards of conduct in cyber space.*[57]

Ketidaksiapan hukum dalam penegakan hukum *cyber crime* ini menyebabkan pencegahan dengan menggunakan teknologi dan budaya menjadi alat yang ampuh. Hal ini terungkap dari korban hacking yang merasa nyaman dengan pendekatan teknologi untuk menanggulangi *cyber crime*. Ketika situs mereka dirusak, mereka menggunakan teknologi dalam memperbaikinya dan mengantisipasinya dengan menggunakan sistem pengamanan yang ketat.

Perkembangan teknologi dan ilmu pengetahuan khususnya mengenai teknologi elektronik telah menimbulkan pengaruh hampir dalam seluruh aspek kehidupan manusia dan kegiatannya di masyarakat, termasuk dalam aspek hukum. Penggunaan teknologi sebagai sarana komunikasi (hubungan) secara global telah menumbuhkan tantangan-tantangan positif bagi kemajuan ilmu pengetahuan itu

---

[57] *Ibid.*,

sendiri baik dalam hubungan masyarakat regional, nasional bahkan internasional. Di samping menimbulkan pengaruh positif juga memiliki sisi gelap manakala dampak dari kemajuan tadi tidak diikuti dengan kemampuan bagaimana cara mengoperasionalkan dan tidak tersedianya pengaturan (perangkat hukum) untuk sebagai pembatasan bagi penggunaan teknologi itu sendiri.

Teknologi elektronik seperti penggunaan komputer dan internet sebagai sarana informasi terlihat nyata telah menjadi kebutuhan masyarakat untuk melakukan berbagai aktifitas dalam pergaulan hidupnya di masyarakat, bahkan teknologi ini sering dikatakan oleh sebagian orang sebagai media tanpa batas (dunia maya). Hal demikian didasarkan atas pengetahuan kita bahwa dimensi ruang (tempat), birokrasi, waktu, dalam hubungannya sesama subjek hukum yang selama ini dilakukan berada di dunia nyata telah dengan mudah (dalam hitungan detik) ditembus oleh teknologi informasi. Fakta demikian dapat kita lihat misalnya ; kebebasan dan kemudahan berbicara (*media teleconfren*), keterbukaan dan tukar menukar informasi dalam dan lintas batas wilayah suatu negara, dan perdagangan bebas atau transaksi-transaksi melalui media elektronik. Dalam kenyataan demikian perkembangan teknologi informasi patut disadarai memiliki dampak bagi hukum yang telah ada dan memerlukan penyesuaian pengaturan lebih lanjut, sehingga penggunaan teknologi sebagai sarana komunikasi global dalam pergaulan masyarakat regional /nasional / internasional tetap berada dalam landasan (legalitas) hukum yang benar.

Kebutuhan akan teknologi Jaringan Komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui Internet pula kegiatan komunitas

komersial menjadi bagian terbesar, dan terpesat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar di dunia bisa diketahui selama 24 jam. Melalui dunia internet atau disebut juga *cyberspace*, apapun dapat dilakukan. Segi positif dari dunia maya ini tentu saja menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia, tetapi dampak negatif pun tidak bisa dihindari, tatkala pornografi marak di media Internet, masyarakat pun tak bisa berbuat banyak.

Di sisi lain pada prakteknya perkembangan penggunaan teknologi informasi telah disalahgunakan oleh sebagian orang tertentu sebagai media untuk melakukan kejahatan. Karena itu, seiring dengan perkembangan teknologi internet, menyebabkan munculnya kejahatan yang disebut dengan *cyber crime* atau kejahatan melalui jaringan internet. Fakta ini dapat kita lihat seperti Kasus Pembobolan Bank BNI Cabang New York, pada tahun 1987 yang telah melakukan transfer yang tidak sah (*unauthorized transfer*) dana milik Bank BNI New York ke City Bank melalui " *transfer electronic payment*" yaitu pada tanggal 31 Desember 1986-debet – US s 9.100.000,- dari AC Bank BNI Pusat Jakarta No. 10957914 transfer ke AC Bank BNI New York No. 544772376, yang selanjutnya di transfer lagi untuk keuntungan kredit bagi rekening di berbagai Bank di Panama City, Brussels Lambert bank, serta Kwong On Bank Hongkong.[58] Transfer tidak sah tersebut telah menyebabkan pengalihan

[58] Yuyun Yulianah, 2000, *Pembuktian Tindak Pidana Cyber Crime*, Cianjur : Fakultas Hukum Universitas Suryakancana. h. 2.

dana dan diterima untuk keuntungan rekening Rudy Demsy (terdakwa) pada berbagai Bank penerima.

Kasus lain adalah penggelapan uang di Bank BRI melalui komputer, Perbuatan pidana ini merupakan kerja sama antara orang luar dengan oknum pegawai BRI Cabang Katamsi Yogyakarta dari tanggal 15 September hingga 12 Desember 1982. Penggelapan tersebut dilakukan dengan cara mentransfer uang melalui kliring, kemudian warkat kliring yang diterima dari kliring tersebut oleh oknum Pegawai BRI secara melawan hukum dan tanpa sepengetahuan bagian kartu dibebankan pada rekening orang lain, bukan ke rekening yang tertulis pada warkat kliring dengan cara membukukan melalui komputer tanpa kartu atau *strook mesin*. Perbuatan ini berlangsung 44 (empat puluh empat kali) yang mencapai jumlah Rp. 815.000.000,- (Delapan ratus lima belas juta rupiah) serta 10.000.000,- (Sepuluh juta rupiah) melalui validasi tunai tanpa dilakukan mutasi atas kartu kredit nasabah Ny. Karlina.[59]

Munculnya beberapa kasus *cyber crime* seperti di Indonesia, misalnya pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer. Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya *cyber crime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi

[59] *Ibid.*, h. 3.

teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

Menurut RM. Roy Suryo, kasus-kasus *cyber crime* yang banyak terjadi di Indonesia setidaknya ada tiga jenis berdasarkan modusnya, yaitu :[60]

1. Pencurian Nomor Kartu Kredit. Menurut Rommy Alkatiry (Wakil Kabid Informatika KADIN), penyalahgunaan kartu kredit milik orang lain di *internet* merupakan kasus *cyber crime* terbesar yang berkaitan dengan dunia bisnis *internet* di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau *on-line*. 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*.
2. Memasuki, memodifikasi atau merusak *homepage* (*hacking*). 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 system perbankan dan merusak data base bank.
3. Penyerangan situs atau *e-mail* melalui virus atau *spamming*. Modus yang paling sering terjadi adalah mengirim virus melalui *e-mail*. Menurut RM. Roy Suryo, di luar negeri kejahatan seperti ini sudah diberi hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya.

Sementara itu As'ad Yusuf memerinci kasus-kasus *cyber crime* yang sering terjadi di Indonesia menjadi lima, yaitu :[61]

a. Pencurian nomor kartu kredit. Contoh ; Pebobolan kartu Kredit melalui Internet yang dilakukan oleh Petrus Pangkur dengan hukuman 1 tahun penjara karena melakukan penipuan dan pemalsuan kertu kredit milik orang lain untuk membeli barang. Pada tahun 2002.

[60] Bistek Warta Ekonomi, *Op. Cit.*, h. 12.
[61] Bistek Warta Ekonomi, *Op. Cit.*, h. 13.

b. Pengambilalihan situs *web* milik orang lain. Salah satu kegiatan yang sering dilakukan oleh *cracker* adalah mengubah halaman web, yang dikenal dengan istilah *deface*. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di Indonesia menunjukkan satu (1) situs web dibajak setiap harinya. Contoh kasusnya antara lain :

- Pembajakan web KPU tahun 2004

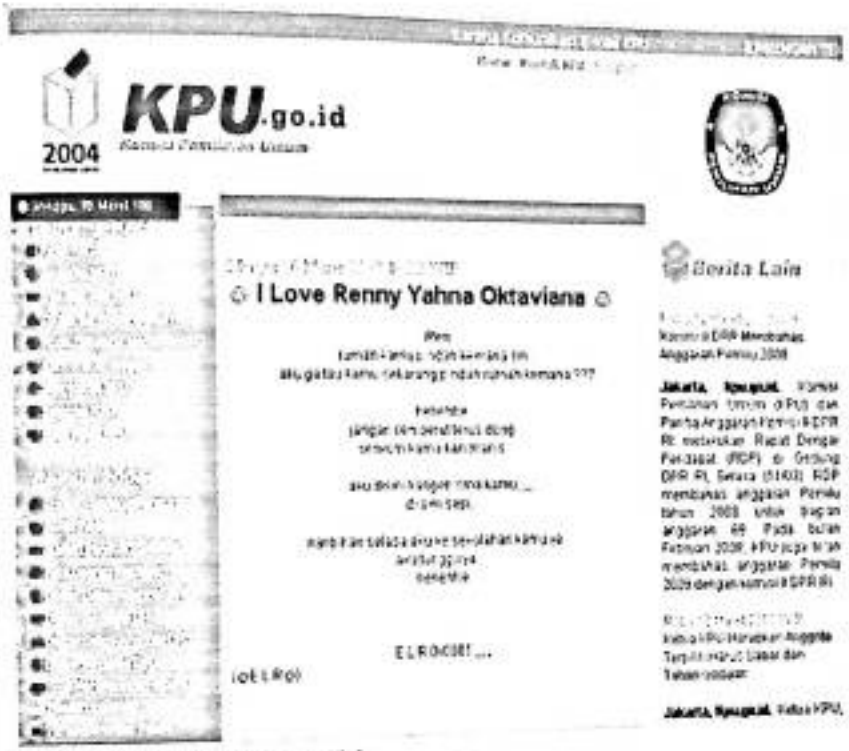
"....Pada hari Sabtu, 17 April 2004, Dani Firmansyah, konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta berhasil membobol situs milik Komisi Pemilihan Umum (KPU) di http://tnp.kpu.go.id dan berhasil melakukan perubahan pada seluruh nama partai disitus TNP KPU pada jam 11:24:16 sampai dengan 11:34:27. Perubahan ini menyebabkan nama partai yang tampil pada situs yang diakses oleh publik, seusai Pemilu Legislatif lalu, berubah menjadi nama-nama lucu seperti Partai Jambu, Partai Kelereng, Partai Cucak Rowo, Partai Si Yoyo,Partai Mbah Jambon, Partai Kolor Ijo, dan lain sebagainya. Dani menggunakan teknik SQL Injection(pada dasarnya teknik tersebut adalah dengan cara mengetikkan string atau perintah tertentu di address bar browser) untuk menjebol situs KPU. Kemudian Dani tertangkap pada hari Kamis, 22 April 2004. Dan sidang kasus pembobolan situs TNP KomisiPemilihan Umum (KPU) digelar Senin(16/8/2004)....."

- Pembajakan web KPU tahun 2009

"....web resmi KPU kpu.go.id Sabtu 15 Maret pukul 20.15 diganggu orang tak bertanggungjawab. Bagian situs kpu.go.id yang diganggu hacker adalah halaman berita, dengan menambah berita dengan kalimat "I Love You Renny Yahna Octaviana. Renny How Are You There?". Bukan hanya itu, sipengganggu juga mengacak-acak isi berita kpu.go.id. pengurus situs web kpu.go.id untuk sementara menutup kpu.go.id /sehingga tidak bias diakses oleh publik yang ingin mengetahui berita-berita tentang KPU khususnya mengenai persiapan Pemilu 2009. Padahal awal April 2008 tahapan awal pelaksanaan Pemilu 2009 yaitu pemutakhiran data pemilih dan pendaftaran Parpol peserta Pemilu mulai dilaksanakan.....

Berikut beberapa contoh gambar situs web yang diserang secara *deface* :

Gambar 2. Pembajakan Situs KPU

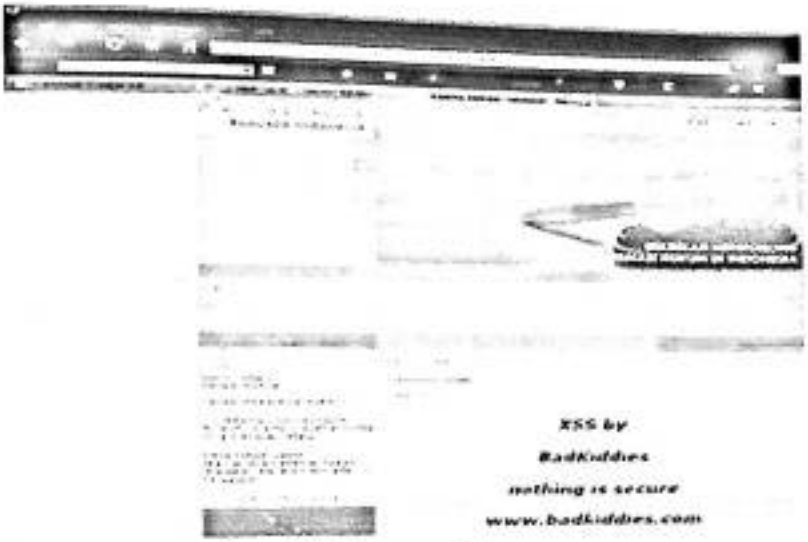


Sumber : www.kpu.go.id

Gambar 3. Pembajakan Situs Depkominfo

Sumber : www.depkominfo.go.id

Gambar 4. Pembajakan situs Komisi Hukum Nasional Republik Indonesia



Sumber : www.komisihukum.go.id

Gambar 5. Pembajakan situs PDAM Kota Denpasar Bali

Sumber : www.denpasarkota.go.id

c. Kejahatan nama *domain.*

Nama domain (*domain name*) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah *cybersquatting*. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk

merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat "domain plesetan", yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah *typosquatting*.

Sementara itu, terdapat juga beberapa kasus *cyber crime* yang terjadi di ruang internasional, seperti :

- Howard Carmack Kirim 825 Juta E-mail,
  Howard Carmack terpaksa mendekam di bui setelah terbukti mengirimkan 825 Juta e-mail sampah menggunakan identitas palsu atau curian. Akibatnya, Howard menerima hukuman tiga setengah tahun penjara dari maksimal tujuh tahun penjara yang dapat didakwakan kepadanya. Graham Cluley, Konsultan Teknologi dari firma Sophos, menyambut baik hukuman tersebut. Setelah Carmack ditangkap, jumlah Spam meningkat drastic. Kasus Howard dimulai dari tuntutan Earthlink, sebuah ISP (Internet Service Provider) di Amerika Serikat. Howard terbukti mengirim e-mail palsu kepada pelanggan EarthLink di Buffalo (salah satu kota di AS). E-mail tipuan itu kemudian digunakan untuk mengambilalih dua rekening e-mail pelanggan Earthlink di Buffalo.[62]
- Kasus Penyebaran Virus Worm,
  Menurut perusahaan software antivirus, worm Randex menyebar dengan cara mendobrak sistem komputer yang tidak diproteksi dengan baik Randex menyebar pada jaringan LAN (local area networks), dan mengeksploitasi komputer bersistem operasi Windows. Menurut perusahaan anti-virus, F-Secure, komputer yang rentan terhadap serangan worm ini adalah komputer-komputer yang menggunakan password yang mudah ditebak. Biasanya hacker jahat menggunakan daftar terprogram untuk melancarkan aksinya. Begitu menginfeksi, worm akan merubah konfigurasi Windows sehingga worm ini langsung beraksi begitu Windows aktif. Worm ini juga menginstal backdoor pada komputer yang disusupinya. Dengan backdoor ini, pembuat worm berkesempatan mengendalikan komputer dari jarak jauh, menggunakan perintah-perintah yang dikirim

[62] Http://www.asphost.com/cyber crime/contohkasus.html diakses pada tanggal 28 Oktober 2009

melalui kanal di IRC (internet relay chat), ungkap penjelasan dari F-Secure.[63]

- Kevin Mitnick Versus Publik AS,
  Di Amerika serikat kejahatan yang dilakukan oleh Kevin Mitnick tentu tidak asing lagi. Sampai sekarang nama Mitnick masih cukup popular bagi kalangan *underground* tanpa kenal batas negara. Kevin Mitnick ditangkap FBI tanggal 15 Februari 1995 dengan tuduhan melakukan beberapa *computer crime* maupun *cyber crime*. Ia sudah mengakui empat kasus *wire fraud*, dua kasus *computer fraud* dan sebuah kasus penyadapan komunikasi lewat kabel. Tidak tanggung-tanggung, ulah mitnick telah memakan korban berbagai perusahaan besar seperti Motorola, Nokia, Fujitsu, Novell, NEC, Sun Microsystems, Colorado SuperNet, Netcom On-Line Services, dan The University of Southern California.[64]
- Pencipta *Spywre Loverspy* Versus Publik AS
  Salah satu ancaman yang tidak kalah bahaya dari worm dan virus adalah *spyware*. Penyebaran *spyware* juga menjadi tindakan mengganggu yang tergolong dalam aksi *cyber crime*. Adalah Carlos Enrique Perez-Melara, pencipta sekaligus penyebar program *spyware* yang diberi nama *Loverspy*. Seperti halnya *spyware, Loverspy* mampu menyusupi system jaringan komputer untuk kemudian menyerap semua informasi yang ada di dalamnya, sesuai dengan kata spy alias mata-mata yang terkandung di dalamnya.[65]

Dari pemaparan kasus-kasus *cyber crime* tersebut di atas dapat disimpulkan bahwa *cyber crime* merupakan permasalahan yang harus ditangani secara serius. Masalah kejahatan mayantara dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama pada perkembangan teknologi informasi masa depan, karena kejahatan ini termasuk salah satu *extra ordinary crime* (kejahatan luar biasa) bahkan dirasakan pula sebagai *serious crime* (kejahatan serius) dan *transnational crime*

---

[63] *Ibid.*,
[64] Mery Magdalena dan Maswigrantoro Roes Setiyadi, 2007, *Cyberlaw, Tidak Perlu Takut*, Yogyakarta : Andi Offset. Hal 99-100
[65] *Ibid.*, Hal 106-107

(kejahatan antar negara) yang selalu mengancam kehidupan warga masyarakat, bangsa dan negara berdaulat. Tindak pidana atau kejahatan ini adalah sisi paling buruk di dalam kehidupan modern dari masyarakat informasi akibat kemajuan pesat teknologi dengan meningkatnya peristiwa kejahatan komputer, pornografi, terorisme digital, "perang" informasi sampah, bias informasi, *hacker*, *cracker* dan sebagainya. Selanjutnya akan dibahas dampak dari perkembangan teknologi informasi terhadap timbulnya *cyber crime*.

B. Kerjasama Internasional Dalam Penanganan *Cyber Crime*

Permasalahan yang ditimbulkan akibat perkembangan teknologi komputer dan informasi, menunjukkan perlu adanya upaya yang menyeluruh untuk menanggulangi *cyber crime*. Kesadaran dari para pengguna jasa internet terhadap *cyberethics* juga akan turut membantu. Selain itu, kerjasama antara negara-negara pengguna jasa internet juga membantu menanggulangi paling tidak mengurangi kejahatan internet yang melintasi batas-batas negara. Mengingat bahwa *cyber crime* tidak mengenal batas-batas negara maka dalam upaya penanggulangannya memerlukan suatu koordinasi dan kerjasama antarnegara. *Cyber crime* memperlihatkan salah satu kondisi yang kompleks dan penting untuk diadakannya suatu kerjasama internasional. Berikut beberapa bentuk kerjasama internasional dalam penanganan *cyber crime* :

C.1. Penanganan *Cyber Crime* Melalui Konvensi *Cyber Crime* di Uni Eropa

Cyber crime merupakan tindak kejahatan transnasional yang melanda banyak negara-negara di dunia khususnya negara-negara maju yang telah menggunakan sistem komputerisasi dan jaringan di hampir semua bidang atau sektor dalam kehidupan berbangsa dan bernegaranya. Kekhawatiran akan masalah keamanan ini dapat terlihat jelas dari kebijakan-kebijakan pemerintah negara menyangkut sistem keamanan jaringan dan data begitu pula dengan perangkat hukumnya yaitu hukum perdata dan pidana yang lebih spesifik mengatur tindak kejahatan ini. Amerika serikat adalah sebagai contoh negara yang memiliki kepentingan yang besar terhadap masalah ini. Kepentingan negara-negara Uni Eropa untuk membangun sistem kerjasama internasional dalam menangani masalah ini terlihat dalam upaya Uni Eropa dalam menyatukan persepsi negara-negara tentang masalah *cyber crime* dalam sebuah konvensi internasional.[66]

Interaksi transnasional adalah interaksi yang paling tinggi intensitas dan frekuensinya dibanding interaksi antar pemerintah yang bersifat kenegaraan. Interaksi transnasional dilakukan oleh masyarakat suatu negara dengan masyarakat di negara lain tanpa ada keterkaitan atau hubungan langsung dengan pemerintah negara, dimana interaksi tersebut meliputi berbagai bidang seperti industri, perusahaan jasa, pendidkan, teknologi, sosial, budaya, politik dan lain sebagainya. Dalam proses

[66] Andi Ahmad Madina, 2003, Prospek Penanganan *Cyber Crime* Dalam Kerangka Kerjasama Keamanan Uni Eropa (Studi Kasus : Konvensi *Cyber Crime*), Universitas Hasanuddin, Fakultas Ilmu Sosial dan Ilmu Politik, Jurusan Hubungan Internasional, Makassar. h. 72.

integrasi, interaksi transnasional yang intensif merupakan syarat mutlak sebagai proses komunikasi antar masyarakat dan sistem yang akan terintegrasi.[67]

Di era revolusi informasi dan komunikasi sekarang ini, interaksi transnasional sebagai bentuk komunikasi menjadi sangat mudah. Internet sebagai teknologi media informasi dan komunikasi yang paling canggih dan cepat telah memberikan banyak perubahan dalam kemajuan peradaban manusia. Internet telah menghapus masalah jarak dan waktu dalam proses interaksi global. Interkasi transnasional dimana dibutuhkan tidak hanya perpindahan pelaku dan barang tetapi juga dituntut adanya perpindahan gagasan dan informasi yang dapat dilakukan dengan sangat cepat melalui internet. Internet telah membuka kebebasan aktor-aktor hubungan internasional baik dari pemerintah maupun non pemerintah untuk dapat berinteraksi dengan lebih intensif dalam pentas global.[68]

Uni Eropa sebagai institusi aliansi integratif yang berlandaskan pada integrasi ekonomi dibentuk atas kesepakatan pemerintah negara-negara anggotanya dan pada prosesnya dibangun dari interaksi transnasional yang terjadi di dalamnya. Media informasi dan komunikasi bagi proses integrasi ekonomi Uni Eropa adalah sangat penting bahkan telah menjadi tulang punggung sistem perekonomian tersebut. Interaksi pelaku ekonomi dalam kawasan Union dan Eropa pada umumnya sangat bergantung pada teknologi informasi dan komunikasi seperti internet.[69]

---

[67] *Loc. Cit.*,
[68] *Ibid.*, h. 73
[69] *Loc. Cit.*,

Usaha negara-negara Eropa dalam menghadapi masalah teknologi komunikasi dan informasi serta *cyber crime* dapat terlihat dengan adanya beberapa kebijakan negara Eropa yang dimulai pada tahun 1988. Kebijakan-kebijakan tersebut berupa kerjasama keamanan sistem informasi dan jaringannya, perlindungan data, *e-commerce*, *electronic signature,* dan infrastruktur keamanan jaringan. Sebelum ditetapkannya pelaksanaan konvensi *cyber crime* telah ada negosiasi di antara negara-negara anggota Uni Eropa pada tingkat *European Council* yang berlangsung mulai pada akhir tahun 1990-an hingga pertengahan 2001.[70]

Konvensi *cyber crime* di desain untuk menerapkan tiga hal yaitu : pertama, menyamakan persepsi tentang definisi tindak kejahatan tersebut di antara negara-negara peserta. Kedua, megajukan standarisasi keamanan transisi dan langkah-langkah prosedur yang harus ditempuh oleh perwakilan negara-negara seperti lembaga hukum dan kepolisian, dan ketiga, melakukan kerjasama antar negara-negara dalam mengumpulkan dan berbagai bukti-bukti tindak kejahatan yang melampui batas-batas negara.[71]

Dari ketiga hal tersebut secara umum dapat ditarik kesimpulan bahwa konvensi ini ditujukan untuk kerjasama global. Namun dalam tataran implementasinya konvensi ini lebih diarahkan pada kawasan Uni Eropa. Hal ini terlihat dalam model pembuatan kebijakan ini yang menurut Keohane dan Nye adalah kerjasama internasional "model klub" yang menurut mereka :

---

[70] *Ibid.*, h. 74.
[71] *Loc. Cit.*,

Beginning with Bretton Woods...key regime of governence have operated like clubs. Cabinet members or equivalent who were working on the same issues, initially from a relatively small number of relatifelly rich countries, get together make rules...Trade ministers dominated GATT; finance ministers ran the IMF; defence ministers met at NATO; ...[72]

Dimana dalam pembuatan kebijakan hanya melibatkan kaum elit dalam hal ini adalah *European Council* yang bersifat rahasia atau tidak transparan bagi negara-negara di luar Uni Eropa dan pihak NGOs. Dengan demikian Uni Eropa menciptakan aturan-aturan tersendiri di wilayahnya dalam menciptakan sistem keamanan jaringan dan data sebagai bagian dari kerjasama keamanan.

C.2. Penanganan *Cyber Crime* Dalam Lingkup Regional ASEAN

Cyber crime ataupun *computer related crime* merupakan suatu bentuk kejahatan transnasional yang dalam penanganannya memerlukan adanya kerjasama keamanan khusus untuk meredam dan mencegah perkembangannya disebabkan sifat unik yang ada di dalamnya. Penanganan *cyber crime* dalam lingkup regional ASEAN merupakan bagian dari program *e-ASEAN* yang nantinya dapat menjadi suatu jaminan bagi kemajuan ICT di kawasan ini secara keseluruhan. Hingga saat ini program tersebut berada dalam tahap pengembangan pada keamanan jaringan secara keseluruhan yang mencakup :[73]

---

[72] Robert Keohane and Joseph Nye, Jr., Introduction, *Governance in a Globalizing World*, Washington : Brooking, 2000, hal. 26. dikutip dari Steven E. Bilet, Ph.D dalam *Transnational Advocacy and the Cyber Crime Convention : A Concideratioan of Lobbying and Global Governance*, The George Washington University, 2002, hal. 3

[73] Olan Rinto, 2007, Prospek Penanganan *Cyber Crime* Dalam Kerangka Kerjasama Keamanan ASEAN, Universitas Hasanuddin, Fakultas Ilmu Sosial dan Ilmu Politik, Jurusan Hubungan Internasional, Makassar. h. 76.

- Pengembangan infrstruktur teknologi informasi dan komunikasi

Pengembangan pada infrasrtuktur teknologi informasi dan komunikasi ini meliputi perluasan jaringan IPv6, *Voice over Internet Protocol* (VoIP), dan *wireless broadband* di kawasan Asia Tenggara. Untuk mempercepat proses pembangunannya ASEAN melakukan beberapa kerjasama dengan negara-negara maupun organisasi di luar ASEAN yang cukup menjanjikan adalah kerjasama dengan Uni Eropa. Beberapa forum ASEAN dan Uni Eropa pada sektor ICT yang telah diadakan diantaranya *The First Euro-Southeast Asia Information and Communications Technology Forum* 2006 (EUSEA 2006) yang diadakan di Singapura pada juni 2006, Second ICT *Research Collaboration Conference* di Jakarta pada september 2006 dan yang terakhir *Euro-Southeast Asia* 2006 ICT Forum pada 21 – 23 November 2006 di Helsinki. Kerjasama ASEAN dengan Uni Eropa dalam pengembangan pada sektor ICT adalah suatu langkah yang tepat disebabkan tingginya tingkat perkembangan ICT dan *cyber security* di Eropa.[74]

- Standarisasi regulasi hukum (*cyber law / cyber policies*)

Dalam pengembangan *cyber security* yang kuat dibutuhkan adanya suatu regulasi atau aturan berupa *cyber law / cyber policies* yang dapat mengatur ruang maya (*cyber space*) ini. Di antara negara-negara ASEAN yang telah memberlakukan undang-undang khusus masalah adalah yang menyangkut *cyber space* ini adalah Singapura (*Computer Misuse Act*), Thailand (*Computer Crime Bill*), Filipina (*Philippines Republic Act No.*8792). Malaysia (*Computer Crimes Act* 1997), dan

[74] *Ibid.*, h. 77

Brunei Darussalam (*Computer Misuse order of 2000*), sedangkan Laos, Kamboja, Myanmar, Vietnam, dan Indonesia masih dalam tahap rancangan undang-undang dan sementara disatukan dengan regulasi tentang telekomuniaksi dan transaksi elektronik. ASEAN melalui *e-ASEAN framework* menyadari pentingnya penerapan regulasi standar menyangkut masalah *cyber security* untuk meningkatkan *e-commerce* secara regional dan meningkatkan kepercayaan dunia terhadap keamanan jaringan yang ada di kawasan ini. *Cyber law* tak hanya terkait dengan keamanan dan kepastian transaksi, tapi juga keamanan dan kepastian berinvestasi di dalam *cyber space*. Dan diharapkan dengan adanya kesepakatan regulasi hukum yang relevan dan kondusif di antara negara-negara ASEAN, maka kegiatan bisnis dapat berjalan dengan kepastian hukum yang memungkinkan menjerat semua *cyber fraud* atau tindakan kejahatan dalam kegiatan bisnis online, maupun yang terkait dengan *cyber crime* pada umumnya.[75]

- Koordinasi dan kerjasama keamanan

Dalam penanganan *cyber crime* dalam hal ini proses penyelidikan dan penindakannya, ASEAN menyerahkan pada ASEANAPOL dan ASEAN CERT's untuk berkoordinasi dan saling bertukar informasi yang sesuai dengan standar prosedur yang telah ditetapkan dan selanjutnya diserahkan kepada interpol untuk menindaklanjutinya. Selain itu juga dalam pengawasan keamanan jaringan internet ASEAN mengadakan kerjasama dengan beberapa negara di luar kawasan ini seperti kerjasama dalam pengawasan jaringan internet bersama negara-negara di Asia Pasifik

[75] *Loc. Cit.*,

yaitu *Internet Security System* (ISS) dengan pusat di Australia *Security Operation Center* (SOC) untuk mengkover wilayah Asia Tenggara dan Australia. Dalam proses penyidikan *cyber crime* terdapat beberapa tahapan yang harus dilalui untuk mendapatkan hasil yang maksimal. Beberapa tahapan itu antara lain tahap pelaporan, tahap penyidikan, tahap pemecahan kasus, dan tahap pengadilan. Pada tahap penyidikan kasus *cyber crime* yakni tahap investigasi kejahatan komputer yang juga dikenal sebagai komputer forensik (*computer forensic*) secara khusus adalah pengumpulan informasi dari komputer dan mengenai sistem komputer yang dapat diterima dalam sebuah pengadilan hukum. Pada tahap peradilan suatu kasus *cyber crime* diperlukan berbagai data yang dapat menetukan yurisdiksi yang akan digunakan untuk menjerat pelaku. Data tersebut antara lain tempat atau lokasi tersangka melakukan aksinya yakni lokasi akses internet, lokasi korban, dan kewarganegaraan tersangka dan korban.[76]

[76] *Ibid.*, h. 79-80

BAB IV

ANALISIS HASIL PENEITIAN

A. Dampak Kejahatan di Internet (*Cyber Crime*) sebagai Kejahatan Transnasional

Perkembangan ilmu pengetahuan dan teknologi yang cukup pesat sekarang ini sudah menjadi realita sehari-hari bahkan merupakan tuntutan masyarakat yang tidak dapat ditawar lagi. Tujuan utama perkembangan iptek adalah perubahan kehidupan masa depan manusia yang lebih baik, mudah, murah, cepat dan aman. Perkembangan iptek, terutama teknologi informasi seperti internet sangat menunjang setiap orang mencapai tujuan hidupnya dalam waktu singkat, baik legal maupun illegal dengan menghalalkan segala cara karena ingin memperoleh keuntungan secara "potong kompas". Dampak buruk dari perkembangan "dunia maya" ini tidak dapat dihindarkan dalam kehidupan masyarakat modern saat ini dan masa depan.

Sistem informasi saat ini merupakan sumber daya dan mempunyai peranan yang sangat penting dalam keberlangsungan dan kompetensi organisasi. Seiring dengan kenyamanan, kemudahan dan keuntungan yang dijanjikan atau ditawarkan dalam setiap pengembangan dan implementasi suatu sistem informasi, disadari menjadikan sistem informasi semakin rentan akan potensi ancaman (threats). Dengan adanya kesadaran tersebut, maka pengelolaan sistem informasi juga harus diimbangi dengan perhatian yang serius terhadap keamanan sistem informasi (information system security). Keamanan sistem informasi merupakan salah satu bagian yang penting dalam melakukan pengelolaan sistem informasi.

Prinsip-prinsip kerahasiaan, integritas dan ketersediaan informasi (*confidentiality, integrity and availability - CIA*) tersebut merupakan taruhan dalam keamanan sistem informasi. Prosedur dan mekanisme keamanan harus mampu menjamin sistem dapat terlindungi dari potensi ancaman yang mungkin timbul. Hasil survey yang dilakukan oleh AT&T ataupun oleh *CSO Magazine, U.S Secret Service,* dan *CERT® Coordination Center*, memperlihatkan atau mengidentifikasi bentuk-bentuk potensi ancaman terhadap sistem informasi, seperti terlihat dalam tabel berikut

Tabel 1. Potensi Ancaman Terhadap Sistem Informasi 2004-2006

Which do you regard as the three most significant security threats to your company today and in two year's time?	2004	2006
Viruses and worms	92%	87%
Hackers	50%	51%
Accidental damage	40%	33%
Spam	36%	31%
Internal sabotage	27%	25%
Power outages	19%	14%
Denial of service attacks	17%	19%
Competitor espionage	12%	17%
Terrorist attacks	9%	15%
Natural disasters	8%	8%
Other Please Specify	1%	2%

Source:AT&T Economic Intelligence Unit Networking and Business Strategy Survey, March-April 2004

Sumber : AT&T Economic Inteligen Unit 2004

Tabel 2. Bentuk Kejahatan Terhadap Sistem Informasi

Types of Electronic Crimes (base: 347)	
Virus or other malicious code	77%
Denial of service attack	44%
Illegal generator of SPAM email	38%
Unauthorized access by an insider	38%
Phishing	31%
Unauthorized access by an outsider	27%
Fraud	22%
Theft of intellectual property	20%
Theft of other proprietary info	16%
Employee identity theft	12%
Sabotage by an insider	11%
Sabotage by an outsider	11%
Extortion by an insider	9%
Extortion by an outsider	9%
Other	11%
Don't know	8%

Sumber : *2004 - 2005 e-Crime Watch Survey*, CSO Magazine, U.S Secret Service, and CERT® Coordination Center.

Dari data hasil survey pada tabel 1 dan 2 tersebut di atas, secara umum terlihat *hackers*, para pegawai aktif dalam organisasi (*current employees*) bahkan konsumen, dianggap atau dapat dipersepsikan sebagai potensi ancaman terhadap sistem informasi. Dalam konteks keamanan sistem informasi, disyaratkan upaya-upaya yang bersifat pencegahan (*prevention*) terhadap potensi ancaman yang mungkin timbul, selain juga upaya pendeteksian kejahatan terhadap sistem informasi dan upaya pemulihan sistem informasi. Pencegahan menjadi penting karena dapat menghindarkan pengelola atau pemilik sistem informasi dari timbulnya kejahatan (*computer related crime*), kerugian yang lebih besar dan upaya atau biaya yang besar dalam upaya deteksi, ditempuhnya proses hukum dan *recovery* terhadap sistem informasi yang telah rusak.

Globalisasi dunia melalui teknologi informasi berkembang sangat pesat. Dampak perkembangan teknologi informasi dirasa sangat berpengaruh terhadap pengaturan hukum. Betapa tidak dengan penggunaan teknologi informasi perilaku manusia secara nyata telah beralih dari model aktifitas yang didasarkan pada suatu bentuk hubungan *face to face* telah bergeser kepada pola hubungan *digitally*. Oleh karena adanya pergeseran demikian, maka tidak mengherankan dalam setiap aspek kehidupan manusia pun mulai menunjukan suatu fenomena baru. Hal ini salah satunya dapat dilihat pada upaya kreasi manusia yang berkaitan dengan bidang ilmu pengetahuan, seni dan sastra.

Adanya penyalahgunaan teknologi informasi yang merugikan kepentingan pihak lain sudah menjadi realitas sosial dalam kehidupan masyarakat moderen

sebagai dampak dari pada kemajuan iptek yang tidak dapat dihindarkan lagi bagi bangsa-bangsa yang telah mengenal budaya teknologi. Teknologi telah menjadi bagian yang tidak terpisahkan dari kehidupan umat manusia dalam dunia yang semakin "sempit" ini. Semua ini dapat dipahami, karena teknologi memegang peran amat penting di dalam kemajuan suatu bangsa dan negara di dalam percaturan masyarakat internasional yang saat ini semakin global, kompetitif dan komparatif. Bangsa dan negara yang menguasai teknologi tinggi berarti akan menguasai "dunia", baik secara ekonomi, politik, budaya, hokum internasional maupun teknologi persenjataan militer untuk pertahanan dan keamanan negara bahkan kebutuhan intelijen.

Munculnya revolusi teknologi informasi dewasa ini dan masa depan tidak hanya membawa dampak pada perkembangan teknologi itu sendiri, akan tetapi juga akan mempengaruhi aspek kehidupan lain seperti agama, kebudayaan, sosial, politik, kehidupan pribadi, masyarakat bahkan bangsa dan negara. Jaringan informasi global atau internet saat ini telah menjadi salah satu sarana untuk melakukan kejahatan baik domestik maupun internasional. Internet menjadi medium bagi pelaku kejahatan untuk melakukan kejahatan dengan sifatnya yang mondial, internasional dan melampaui batas ataupun kedaulatan suatu negara. Semua ini menjadi motif dan modus operandi yang amat menarik bagi para penjahat digital. Manifestasi kejahatan mayantara yang terjadi selama ini dapat muncul dalam berbagai macam bentuk atau varian yang amat merugikan bagi kehidupan masyarakat ataupun kepentingan suatu bangsa dan negara pada hubungan internasional.

Kejahatan mayantara dewasa ini mengalami perkembangan pesat tanpa mengenal batas wilayah negara lagi (*borderless state*), karena kemajuan teknologi yang digunakan para pelaku cukup canggih dalam aksi kejahatannya. Para *hacker* dan *cracker* bisa melakukannya lewat lintas negara bahkan di negara-negara berkembang aparat penegak hukum, khususnya kepolisian tidak mampu untuk menangkal dan menanggulangi disebabkan keterbatasan sumber daya manusia, sarana dan prasarana teknologi yang dimiliki. Namun perkembangan teknologi digital tidak akan dapat dihentikan oleh siapapun, karena telah menjadi "kebutuhan pokok" manusia moderen yang cenderung pada kemajuan dengan mempermudah kehidupan masyarakat melalui komunikasi dan memperoleh informasi baru.

Dampak buruk teknologi menjadi pekerjaan rumah bersama yang merupakan sisi gelap dari perkembangan teknologi yang harus ditanggulangi. Mengingat kemajuan teknologi telah merambah ke pelosok dunia, termasuk kepedesaan, maka dampak buruk teknologi yang menjadi kejahatan mayantara pada masa depan harus ditanggulangi dengan lebih hati-hati, baik melalui sarana penal maupun non penal agar tidak menjadi masalah kejahatan besar bagi bangsa dan negara yang mengalami krisis ekonomi.

Informasi berikut memperlihatkan *ranking* negara-negara tempat asalnya berbagai program-program pengrusak (baca: *malware*) yang bertujuan menyerang sistem komputer atau teknologi informasi di dunia maya.

Gambar 6. Profil Negara-Negara dengan Program Perusak Dunia Maya

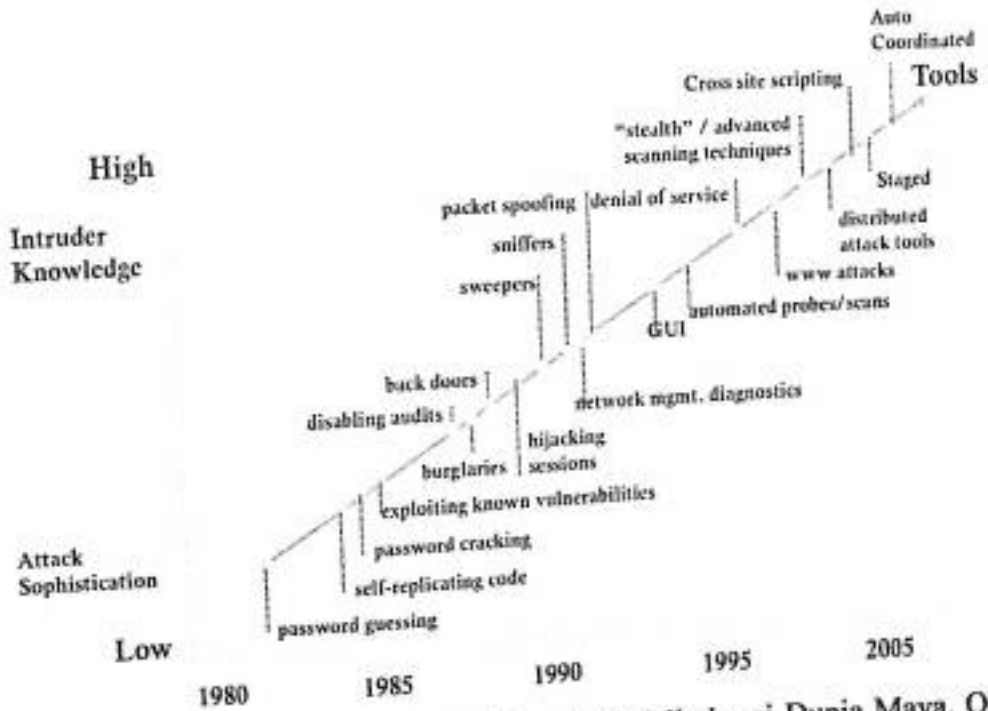
Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	37%	1	1	1	1	1	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10

Sumber : *Cyber* 6. Enam Aspek Menjaga dan Melindungi Dunia Maya. Oleh Prof. Richardus Eko Indrajit

Sejalan dengan kemajuan teknologi komunikasi dan informasi, semakin kompleks pula jenis serangan yang terjadi di dunia maya. Jika dahulu diperkenalkan istilah *hacker* dan *cracker* yang menunjuk pada individu dengan kemampuan dan aktivitas khusus memasuki sistem komputer lain untuk beraneka ragam tujuan, maka saat ini sudah banyak diciptakan mesin atau sistem yang dapat bekerja sendiri secara intelijen untuk melakukan tekniknteknik penyusupan dan perusakan sistem. Intinya adalah bahwa serangan terhadap sistem keamanan teknologi informasi organisasi telah masuk pada kategori kriminal, baik yang bersifat pidana maupun perdata.

Walaupun kebanyakan jenis tindakan kriminal tersebut berkaitan erat dengan urusan finansial, tidak jarang akibat serangan tersebut, sejumlah nyawa manusia melayang, karena menimpa sistem yang sangat vital bagi kehidupan manusia. Ilustrasi berikut memperlihatkan begitu banyaknya jenis tindakan atau serangan yang mengarah pada kriminalisasi dari tahun ke tahun.

Gambar 7. Jenis-Jenis Serangan yang Mengarah pada Kriminalisasi



Sumber : *Cyber* 6. Enam Aspek Menjaga dan Melindungi Dunia Maya. Oleh Prof. Richardus Eko Indrajit

Studi mendalam mengenai tindakan kriminal di dunia maya memperlihatkan berbagai motif atau alasan seseorang melakukannya, mulai dari mencari sensasi semata hingga dibiayai oleh sekelompok sponsor teroris internasional. Hampir seluruh negara melaporkan bahwa tindakan kriminal di dunia maya menunjukkan

pertumbuhan yang semakin signifikan, baik dilihat dari sisi kuantitas maupun kualitasnya.

B. Kendala-kendala Penanganan *Cyber Crime* dalam Kerjasama Internasional

Cyber crime pada dasarnya adalah penyalahgunaan komputer dengan cara *hacking* komputer ataupun dengan cara-cara lainnya sehingga merupakan kejahatan yang perlu ditangani dengan serius. Dikarenakan kejahatan ini potensial menimbulkan kerugian pada beberapa bidang : politik, ekonomi, sosial budaya yang siginifikan dan lebih memprihatinkan dibandingkan dengan ledakan bom atau kejahatan yang berintensitas tinggi lainnya bahkan di masa akan datang dapat mengganggu perekonomian nasional melalui jaringan infrastruktur yang berbasis teknologi elektronik (perbankan, telekomunikasi satelit, jaringan listrik, dan jaringan lalu lintas penerbangan). Karena itu, dalam mengantisipasi hal ini perlu rencana persiapan yang baik sebelumnya.

Secara umum penguasaan operasional komputer dan pemahaman terhadap *hacking* atau penyerangan komputer serta kemampuan melakukan penyidikan terhadap kasus-kasus tersebut dari para penyidik masih sangat minim. Terdapat kendala-kendala berupa faktor pendorong dan penghambat yang mempengaruhi hal tersebut dalam kerjasama penanganan *cyber crime*. Namun dari beberapa faktor tersebut ada yang sangat berpengaruh (determinan) dalam menanggulangi kejahatan dunia maya tersebut.

Berikut beberapa faktor yang menjadi pendorong lajunya pertumbuhan kerjasama penanganan *cyber crime*, antara lain adalah :

1. Kesadaran Hukum Masyarakat. Proses penegakan hukum pada dasarnya adalah upaya mewujudkan keadilan dan ketertiban di dalam kehidupan bermasyarakat. Melalui sistem peradilan pidana dan sistem pemidanaan. *Cyber Crime* adalah sebuah perbuatan yang tercela dan melanggar kepatutan di dalam masyarakat serta melanggar hukum, sekalipun sampai sekarang sukar untuk menemukan norma hukum yang secara khusus mengatur *cyber crime*. Oleh karena itu, peran masyarakat dalam upaya penegakkan hukum terhadap *cyber crime* adalah penting untuk menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan *cyber crime*.

2. Faktor Keamanan. Rasa aman tentunya akan dirasakan oleh pelaku kejahatan (*cyber crime*) pada saat sedang menjalankan aksinya. Hal ini tidak lain karena internet lazim dipergunakan ditempat-tempat tertutup, seperti di rumah, kamar, tempat kerja, perpustakaan, bahkan warung internet (warnet). Aktivitas yang dilakukan yang dilakukan oleh para pelaku di tempat-tempat tersebut sulit untuk diketahui oleh pihak luar. Akibatnya, pada saat pelaku sedang melakukan tindak pidana atau kejahatan sangat jarang orang luar yang mengetahuinya. Hal ini sangat berbeda dengan kejahatan-kejahatan yang sifatnya konvesional, yang mana pelaku akan mudah diketahui secara fisik ketika sedang melakukan aksinya.

3. Faktor Penegak hukum. Faktor penegak hukum sering menjadi penyebab maraknya kejahatan dunia maya (*cyber crime*). Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum mengalami kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku, terlebih apabila kejahatan yang dilakukan memiliki sistem pengoperasian yang sangat rumit. Di samping itu, aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak institusi kepolisian yang belum dilengkapi jaringan internet.

4. Faktor ketiadaan Undang-undang. Perubahan-perubahan sosial dan perubahan-perubahan hukum tidak selalu berlangsung secara bersama sama, artinya pada keadaan-keadaan tertentu perkembangan hukum mungkin tertinggal oleh perkembangan unsur-unsur lainnya dimasyarakat. Begitu juga dengan perkembangan hukum ditengah kemajuan teknologi informasi sangat dirasakan jauh tertinggal.

Selain itu, faktor yang menjadi hambatan dalam kerjasama menangani *cyber crime* sebenarnya sederhana saja. Di Indonesia misalnya, masih sedikit penegak hukum yang memahami perkembangan kejahatan. Namun hal tersebut merupakan kondisi yang umum terjadi di negara-negara yang baru mengenal teknologi internet, dan keberadaan undang-undang (hukum positif) di Indonesia telah mengalami

stagnan. Karena tidak berlaku secara luas dalam arti mampu iuntuk mencegah (meredam) kejahatan baru.

Secara detil, di Indonesia memiliki permasalahan mendasar dalam pengembangan hukum. Sehingga permasalahan *cyber crime* masih menjadi isu elit di kalangan praktisi teknologi informasi. Selain itu, di Indonesia sendiri masih memiliki permasalahan dengan penerapan hukum. Kitab Undang-Undang Hukum Acara Pidana Indonesia tidak di desain untuk kejahatan berbasis teknologi informasi. Akhirnya, *cyber crime* akan menjadi sulit untuk dibuktikan dan pelakunya sulit untuk diberikan sanksi.

Adapun faktor-faktor penghambat yang mempengaruhi kerjasama penanganan *cyber crime* adalah sebagai berikut:

a. Kurangnya pengetahuan tentang komputer dan sebagian besar dari mereka belum menggunakan Internet atau menjadi pelanggan pada salah satu ISP (Internet Service Provider).
b. Pengetahuan dan pengalaman para penyidik dalam menangani kasus-kasus cyber crime masih terbatas. Mereka belum mampu memahami teknik hacking, modusmodus operandi para hacker dan profil-profilnya.
c. Faktor sistem pembuktian yang menyulitkan para penyidik karena Jaksa (PU) masih meminta keterangan saksi dalam bentuk Berita Acara Pemeriksaan (BAP) formal sehingga diperlukan pemanggilan saksi/korban yang berada di luar negeri untuk dibuatkan berita acaranya di Indonesia ,

belum bisa menerima pernyataan korban atau saksi dalam bentuk faksimili atau email sebagai alat bukti

Selain itu, terdapat juga 4 Aspek yang menjadi faktor penghambat kerjasama dalam penanganan *cyber crime* yang terdiri atas :

1. Aspek Yuridis

Penerapan pasal yang disangkakan terhadap tersangka masih menjadi persoalan karena berkaitan dengan teknologi atau jaringan akses komunikasi. Korban pemilik kartu kredit atau perusahaan pengeluar belum dapat diperiksa karena berada di luar negeri.

2. Aspek Teknologi

Kesulitan penyidik karena kemampuan akan komputer terbatas (khususnya dalam internet), cara kerja siklus pemesanan melalui internet, sehingga pendistribusian barang berlangsung secara otomatis.

3. Aspek Perekonomian

Mengganggu terhadap perdagangan yang dilakukan oleh para pelaku asing, hilangnya kepercayaan negara produsen terhadap negara pemesan (contoh, negara Hongaria)

4. Aspek Hubungan Internasional

Kepercayaan terhadap para pengusaha hilang, pajak pemasukan untuk negara menurun.

C. Prospek Kerjasama Internasional dalam Penanganan *Cyber Crime*

Permasalahan yang ditimbulkan akibat perkembangan teknologi komputer dan informasi, menunjukkan perlu adanya upaya yang menyeluruh untuk menanggulangi *cyber crime*. Kesadaran dari para pengguna jasa internet terhadap *cyberethics* juga akan turut membantu. Selain itu, kerjasama antara negara-negara pengguna jasa internet juga membantu menanggulangi paling tidak mengurangi kejahatan internet yang melintasi batas-batas negara.

Namun demikian, kebebasan *cyber* dalam aktivitas internet itu haruslah dilakukan sedemikian rupa sehingga tidak merugikan kepentingan umum atau konsumen, melanggar hak pribadi orang lain, mengganggu keamanan nasional, mengancam integritas bangsa serta melanggar nilai dan norma kesusilaan dan moralitas. *Cyberliberty* dalam internet dapat dipakai sebagai media yang efektif untuk melancarkan ancaman internet (*cyberthreat*). *Cyberliberty* juga memudahkan orang melakukan kejahatan yang merusak moralitas, nilai dan norma seperti perjudian, prostitusi maupun pornografi.

Cyber crime merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh kehidupan modern saat ini. Sehubungan dengan hal tersebut, kejahatan dunia maya jelas bersifat lintas batas negara (*borderless*). Jadi, *cyber crime* bukan hanya masalah nasional tapi juga masalah internasional.

Cyber crime merupakan masalah internasional, maka diperlukan upaya hukum internasional dalam mengantisipasi masalah *cyber crime*. Perkembangan dalam

hukum internasional sendiri memang telah menunjukkan bahwa telah dilakukan berbagai upaya kerjasama internsional dalam mengantisipasi *cyber crime*. Akan tetapi, instrumen hukum internasional di bidang *cyber crime* merupakan sebuah fenomena baru dalam tatanan modern mengingat *cyber crime* sebelumnya tidak mendapat perhatian dari negara-negara sebagai subyek hukum internasional. Munculnya bentuk kejahatan baru yang tidak saja bersifat lintas batas tetapi juga terwujud dalam tindakan-tindakan virtual telah menyadarkan masyarakat internasional tentang perlunya perangkat hukum internasional baru yang dapat digunakan sebagai kaidah hukum internasional dalam mengatasi kasus-kasus *cyber crime*..

Telah banyak contoh bentuk kejahatan yang terjadi di dunia maya, seperti kasus-kasus mafia *cyber* yang merebak pertengahan tahum 2004 di Amerika Serikat. Lalu di Indonesia sendiri pernah mengalami, ketika sistem jaringan Komisi Pemilihan Umum (KPU) pada tahun 2004 disusupi oleh para *hacker*. Hal ini tentu saja mencemaskan karena ketika dunia semakin tergantung kepada teknologi dan manajemen berbasis pada informasi, ternyata kemajuan dalam penanggulangan kejahatan berbasis teknologi ini dapat dikatakan berjalan perlahan. Penanggulangan *cyber crime* oleh nagara-negara secara bersama sangatlah penting dilakukan, terutama kerjasama internasional yang menyelenggarakan pengawasan dan pengontrolan *cybercrime*. Sesungguhnya *cyber crime* sangat mengganggu terutama bagi negara-negara maju yang kebanyakan system administrasinya menggunakan sistem internet.

Di kawasan Uni Eropa telah dibuat suatu strategi *Council of Europe* yang akan memanfaatkan kebutuhan dan dukungan kerjasama internasional dalam menghadapi masalah *cyber crime* sebagai pendorong kerjasama keamanan jaringan internet dan data di kawasan tersebut. Dimana di Budapest, Hongaria, 30 negara sepakat untuk menandatangani *Convention on Cybercrime* yang merupakan kerjasama multilateral yang diadakan guna menanggulangi penyebaran aktivitas kriminal melalui internet dan jaringan komputer lainnya. Melalui kerjasama ini diharapkan dapat menggugah masyarakat internasional untuk ikut berpartisipasi dalam penanggulangan kejahatan berteknologi tinggi Akan tetapi, strategi tersebut tidak mencapai hasil yang diharapakan yaitu dukungan negara-negara EU-15 atau konvensi ini dengan meratifikasikannya. Hal ini disebabkan karena besarnya benturan kepentingan Uni Eropa dengan kepentingan perlindungan politik atau industri yang ujungnya berakhir pada kedaulatan negara dalam mengontrol sistem jaringan informasi dan komunikasinya.

Terciptanya suatu jaringan internet yang aman, nyaman, dan terjangkau dapat dicapai dengan menerapkan beberapa cara salah satunya adalah pengawasan atau kontrol terhadap aktivitas di dalam *cyber space*. Dalam mengawasi dan mengkontrol arus informasi yang ada di internet dapat digunakan suatu cara yakni *content control* atau kontrol terhadap akses informasi yang dianggap dapat merusak ataupun mengancam kehidupan negara seperti yang dilakukan oleh China dalam mengontrol generasi mudanya dari pengaruh globalisasi. *Content control* seperti ini dapat dilakukan dengan cara memblokir akses situs –situs yang dianggap sensitive, akan

tetapi hal ini cenderung tidak sesuai dengan adanya budaya yang ada seperti di Asia Tenggara. Sebagai contoh, di ASEAN terdapat negara-negara yang tidak memberlakukan *content control* (*no content control*) adalah Indonesia, Kamboja, dan Philippinies. Adapun di ASEAN yang telah memberlakukan *content control* adalah singapura (*firewall to pornographic sites, registration of content providers*), Vietnam (*firewall, registration of content providers*), Laos dan Malaysia.

Penerapan *content control* menimbulkan pro dan kontra menyangkut hak kebebasan individu untuk mendapatkan informasi dalam kasus ini informasi yang terdapat di internet. Selain itu pula pengawasan terhadap aktivitas di dalam *cyber space* dapat dilakukan dengan metode *log data report* yang mencatat setiap aktivitas pengguna internet, namun metode ini cenderung sulit untuk diterapkan di ASEAN disebabkan sebagaian besar negara-negara di ASEAN masih belum mempunyai kapasitas regulasi yang dapat mengatur proses pencatat data tersebut secara rutin. Di samping itu juga metode tersebut memerlukan biaya dan infrastruktur teknologi yang cukup tinggi.

Selain itu, di Indonesia dan Singapura telah membuat *cyber law* untuk mencegah adanya *cyber crime* di negara mereka masing-masing. RUU *Cyber Crime* di negara Singapura disebut RUU ETA atau *The Electronic Transactions Act* dan Indonesia membentuk RUU *Cyber Crime* yang disebut RUU ITE atau Informasi dan Transaksi Elektronik. ETA (*The Electronic Transactions Act*) sebagai pengatur otoritas sertifikasi di Singapura, negara tersebut mempunyai misi untuk menjadi pusat kegiatan perdagangan elektronik internasional, di mana transaksi perdagangan yang

elektronik dari daerah dan di seluruh dunia diproses. *The Electronic Transactions Act* yang telah ditetapkan tanggal 10 Juli 1998 yang lalu diciptakan dalam kerangka yang sah tentang undang-undang untuk transaksi perdagangan elektronik di Singapura yang memungkinkan bagi Menteri Komunikasi Informasi dan Kesenian untuk membuat peraturan mengenai perijinan dan peraturan otoritas sertifikasi di Singapura.

Akan tetapi dari semua negara di dunia yang telah melakukan upaya penanganan *cyber crime* ini menemukan masalah dalam perihal yurisdiksi. Pengertian yurisdiksi sendiri adalah kekuasaan atau kompetensi hukum negara terhadap orang, benda atau peristiwa (hukum). Yurisdiksi ini merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak campur tangan. Yurisdiksi juga merupakan suatu bentuk kedaulatan yang vital dan sentral yang dapat mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum.

Dalam kegiatan *cyber space*, yurisdiksi di *cyber space* membutuhkan prinsip-prinsip yang jelas yang berakar dari hukum internasional. Hanya melalui prinsip-prinsip yurisdiksi dalam hukum internasional, negara-negara dapat dihimbau untuk mengadopsi pemecahan yang sama terhadap pertanyaan mengenai yurisdiksi internet. Hal ini dapat ditafsirkan bahwa dengan diakuinya prinsip-prinsip yurisdiksi yang berlaku dalam hukum internasional dalam kegiatan *cyber space* oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasana dalam rangka harmonisasi ketentuan-ketentuan pidana untuk menanggulangi *cyber crime*.

Prospek penanganan *cyber crime* dalam kerangka kerjasama keamanan interasional ini diharapkan akan dapat mendukung kerjasama internasional dalam

memajukan perekonomian di seluruh Negara pada khususnya. Dengan terciptanya suatu jaminan sekuritas jaringan teknologi informasi dan komunikasi akan mendorong pertumbuhan *e-commerce* secara keseluruhan di tiap-tiap negara. Melihat peningkatan jumlah pemakai internet yang cukup pesat di beberapa negara di dunia seperti Vietnam dan Myanmar serta Amerika menunjukkan adanya peningkatan minat masyarakat di seluruh negara terhadap manfaat dari kemajuan teknlogi informasi dan komunikasi ini. Di samping itu juga, peningkatan jumlah pemakai internet juga akan memperbesar peluang terjadinya kasus-kasus *cyber crime* yang patut diwaspadai oleh negara-negara di dunia dalam membangun *cyber security*.

Penanganan *cyber crime* melalui kerangka kerjasama internasional memerlukan partisipasi yang tidak hanya dari pemerintah masing-masing negara saja akan tetapi juga keterlibatan masyarakat dan perusahaan-perusahaan swasta khusunya untuk mendukung terciptanya *cyber security* yang dapat melindungi semua lapisan masyarakat. Dukungan dari perusahaan-perusahaan swasta khususnya perusahaan asing sudah cukup terlihat dari beberapa kerjasama yang dilakukan oleh *vendor-vendor software* seperti *Microsoft* yang mendukung pemerintah untuk mengurangi pembajakan *software*, sedangkan *vendor-vendor* antivirus seperti *Kaspersky* juga telah membangun pusat keamanan jaringan di Indonesia baru-baru ini. Begitu pula dengan beberapa perusahaan manufaktur hardware yang mengadakan beberapa event dalam bentuk pameran maupun pelatihan untuk memajukan perkembangan ICT di kawasan ini. Bantuan-bantuan ini sudah sepatutnya menjadi perhatian pemerintah di masing-masing negara seluruh dunia untuk dapat dimanfaatkan secara maksimal.

Prospek penanganan *cyber crime* dalam kerangka kerjasama keamanan internasional merupakan suatu hal yang sangat bergantung pada persiapan dan patisipasi masing-masing negara dalam menghadapi tatangan globalisasi informasi di masa datang. Diharapkan dengan terbentuknya suatu jaringan internet yang aman, nyaman, dan terjangkau akan meningkatkan kepercayaan masyarakat dunia akan pentingnya kerjasama internasional dalam penanggulangan *cyber crime*. Penanganan secara profesional dan terorganisir pada kasus-kasus cyber crime akan memberikan nilai tambah dan juga dapat memulihkan reputasi sistem keamanan internasional yang cukup memprihatinkan dalam penanganan masalah sekuritas jaringan teknologi informasi dan komunkasi ini.

BAB V

PENUTUP

A. Kesimpulan

1. Teknologi informasi dan komunikasi telah mengubah perilaku dan pola masyarakat global. Perkembangan teknologi informasi telah pula menyebabkan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, budaya, ekonomi, dan pola penegakan hukum. Sejalan dengan itu teknologi informasi semakin memegang peranan penting dalam kehidupan, dan telah membawa sejumlah manfaat. Akan tetapi, disamping segala kemudahan yang ditimbulkan oleh kolaborasi antara penemuan komputer dan penyebaran informasi melalui komputer sehingga melahirkan apa yang dikenal dengan istilah internet (*interconcting network*), berdampak pada munculnya potensi kejahatan baru yang disebut *cyber crime*. *Cyber crime* pada saatnya akan menjadi bentuk kejahatan serius yang dapat membahayakan keamanan individu, masyarakat dan negara serta tatanan kehidupan global. Karena itu munculnya revolusi teknologi informasi dewasa ini dan masa depan terhadap timbulnya *cyber crime* hanya membawa dampak pada perkembangan teknologi itu sendiri dan juga akan mempengaruhi aspek kehidupan lain seperti agama, kebudayaan, sosial, politik, kehidupan pribadi, masyarakat bahkan bangsa dan negara.
2. Salah satu aspek yang sangat penting dalam perumusan kerangka sistematik guna pencegahan dan penanggulangan kejahatan transnasional khususnya kejahatan

dunia maya atau *cyber crime* adalah menyangkut mekanisme kerjasama internasional. Sebagaimana kita pahami bersama perbedaan dalam kepentingan politik, sistem hukum, bahasa dan kebudayaan diantara berbagai negara merupakan kendala-kendala berupa faktor-faktor pendorong dan penghambat dalam kerjasama penanganan *cyber crime* yang menyebabkan kontribusi terhadap sulitnya tercipta mekanisme kerjasama yang ideal. Terdapat beberapa faktor yang menjadi pendorong dalam kerjasama penanganan *cyber crime* antara lain ; kesadaran hukum masyarakat, faktor keamanan, faktor penegak hukum, dan faktor ketiadaan undang-undang. Adapun faktor-faktor penghambat dalam kerjasama penanganan *cyber crime* yakni ; kurangnya pengetahuan tentang komputer, pengetahuan dan pengalaman para penyidik dalam menangani kasus *cyber crime* masih terbatas, dan faktor sistem pembuktian. Oleh karena itu, dalam mengatasi faktor-faktor tersebut dapat dilakukan berupa bantuan teknis, pelatihan, penyediaan fasilitas sampai dengan pertukaran informasi yang diperlukan serta harmonisasi ketentuan-ketentuan hukumnya pada setiap negara.

3. Pengembangan mekanisme kerjasama internasional, baik dalam lingkup global, regional maupun bilateral harus terus dilakukan guna pencegahan dan penanggulangan kejahatan transnasional. Mengingat bahwa *cyber crime* tidak mengenal batas-batas negara maka dalam upaya penanggulangannya memerlukan suatu koordinasi dan kerjasama antarnegara. *Cyber crime* memperlihatkan salah satu kondisi yang kompleks dan penting untuk diadakannya suatu kerjasama internasional oleh karena kejahatan ini adalah merupakan salah satu kejahatan

baru yang beraspek internasional dan global. Meski demikian efektivitas dan efisiensi pelaksanaannya masih perlu dicari format yang tepat, karena seperti kasus-kasus sebelumnya banyak konvensi internasional yang terbentur dalam pelaksanaannya. Salah satu unsur yang akan menjadi tantangan dalam menerapkan suatu konvensi adalah perbedaan persepsi terhadap masalah yang bermuara dari perbedaan kepentingan dan pengalaman. Apalagi di dalam *cyber crime* ketiadaan batas dalam menanggulanginya merupakan hal baru dalam sejarah penegakan hukum. Karena itu, dibutukan persiapan-persiapan yang matang yang nantinya diharapkan akan mampu menghadapi tantangan globalisasi teknologi informasi melalui kerjasama internasional.

B. Saran

Dalam kerangka kepentingan kerjasama keamanan internasional hendaknya lebih menitikberatkan dalam mencapai kesepakatan dibandingkan dengan mengglobalkan ide-ide yang muncul untuk kepentingan union. Karena setiap negara lebih memiliki persamaan kepentingan yaitu perlindungan keamanan aktivitas perekonomian di kawasan setiap negara serta adanya komitmen dari tiap-tiap negara untuk lebih memajukan proses integrasi.

Selain itu, perlu diperhatikan bahwa dalam menciptakan suatu jaringan teknologi informasi dan komunikasi khususnya internet diperlukan adanya suatu kesepakatan dalam standarisasi proses penanganannya hingga nantinya tidak menimbulkan konflik yang dapat menggagalkan kerjasama yang telah dibangun selamanya. Dengan adanya standarisasi operasi dalam pengawasan *cyber space* maka

setiap negara memiliki pedoman khusus dalam mencegah dan menindak setiap kasus-kasus *cyber crime* yang melibatkan warga negaranya. Dan juga diharapkan adanya keterbukaan dan transparansi dalam proses penyidikan terhadap kasus-kasus *cyber crime*.

Bagi negara-negara yang belum memiliki kemampuan yang cukup baik dari segi teknologi dan perangkat hukum seperti Indonesia, hendaknya mempersiapkan diri dengan menciptakan sistem ketahanan nasionalnya dalam bentuk perundang-undangan yang menyangkut tindak kejahatan komputer dan internet, serta meratifikasi perjanjian-perjanjian internasional tentang perlindungan data dan warga negara menyangkut media informasi dan komunikasi. Hal ini sangat perlu dilakukan agar tidak sampai terjebak dalam permasalahan kriminalitas yang menggunakan teknologi ini baik yang dilakukan oleh individu dan kelompok ataupun negara.

DAFTAR PUSTAKA

Buku-buku

Arief, Barda Nawawi. 1998. *Beberapa Aspek Kebijakan Penegakan dan Pengembangan Hukum Pidana*. PT Citra Aditya Bakti : Bandung..

Baylis, John. 1998. *The Globalization of World Politics : An Introduction To International Relation*. Oxford University, Press Inc : New York.

Booth, Ken and Steve Smith. 1995. *International Relations Theory Today*. Penn State : New York.

Daugherty, James E. and Robert L Pfaltzgraff. 1997. *Contending Theories of International Relations : A Comprehensive Survey*. Longman : New York.

Edison, Jamli. 2005. *Kewarganegaraan*. Bumi Akasara : Jakarta.

Eoghan, Casey. 2001. *Digital Evidence and Compute Crime*. A Harcourt Science and Technology Company : London.

Grabosky, P.N and Russell G. Smith. 1998. *Crime in the Digital Age : Controlling Telecommunications and Cyberspaces Illegalities*. Transaction Publishers : New Brunswick.

Graner, Bryan A, 2004. *Black's Law Dictionary Eighth Edition*. St. Paul : West Thomson.

Holsti, KJ. 1995. *The state, war, and the state of war*. Cambridge University Press.

Kadir, Abdul dan Terra Ch, Triwahyuni. 2003. *Pengenalan Teknologi Informasi*, Yogyakarta : Andi Offset.

Krsna. 2005. *Pengaruh Globalisasi Terhadap Pluralisme Kebudayaan Manusia di Negara Berkembang*. Public Jurnal : Jakarta..

Magdalena, Mery dan Maswigrantoro Roes Setiyadi. 2007. *Cyberlaw, Tidak Perlu Takut*. Andi Offset : Yogyakarta.

Makarim, Edmon. 2005. *Pengantar Hukum Telematika : Suatu Kompilasi Kajian*. PT.Raja Grafindo Persada : Jakarta.

Mansur, Dikdik M Arief dan Elisatris Gultom. 2005. *Cyber Law: Aspek Hukum Teknologi Informasi.* PT. Refika Aditama : Bandung.

Microsoft, 2003, *Encarta Dictionary Tools*, 2003, Microsoft Corporation.

Mursito, Danan dkk. 2005. *PendekatanHukum Untuk Keamanan Dunia Cyber Sera Urgensi Law Bagi Indonesia.* Universitas Indonesia Fakultas Ilmu Komputer : Jakarta.

Plano, Jack C and Roy Olton. 1982. *The Internatinal Relations Dictionary*, Clio Press Ltd : Montana.

Rosenau, James N. 1990. *Turbulence In World Politics, A Theory Of Change And Continuity*. Harvester : New York.

Stephenson, Peter. 2000. *Investigating Computer-Related Crime : A Hanbook For Corporate Investigators*. CRC Press : London New York Washington D.C.

Tunkin, G.I. 1986. *International Law*. Progress Publisher : Moscow.

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

Wisnubroto. 1999. *Kebijakan hukum pidana dalam penanggulangan penyalahgunaan computer*. Universitas Atma Jaya : Yogyakarta.

Yulianah, Yuyun. 2000. *Pembuktian Tindak Pidana Cyber Crime.* Fakultas Hukum Universitas Suryakancana : Cianjur.

Skripsi, Artikel, Karya Ilmiah, Dokumen dan Internet

Ahmad Madina,Andi, 2003, *Prospek Penanganan Cyber Crime Dalam Kerangka Kerjasama Keamanan Uni Eropa (Studi Kasus : Konvensi Cyber Crime)*, Universitas Hasanuddin, Fakultas Ilmu Sosial dan Ilmu Politik, Jurusan Hubungan Internasional, Makassar.

Hamzah, Andi. *Aspek-Aspek Pidana di Bidang Komputer*, 1998.

Ramli, Ahmad M. *Perkembangan Cyber Law Global dan Implikasinya Bagi Indonesia*, Makalah Seminar *The Importance of Information System security in E-Goverrment*, Tim Koordinasi Telematika Indonesia, Jakarta, 28 Juli 2004

Rinto Olan, 2007, Prospek Penanganan *Cyber Crime* Dalam Kerangka Kerjasama Keamanan ASEAN, Universitas Hasanuddin, Fakultas Ilmu Sosial dan Ilmu Politik, Jurusan Hubungan Internasional, Makassar.

James A. Lewis (a), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," *Center of Strategic & International Studies* (December 2002) : 1

James A. Lewis (b), "Internet and Terrorism," *Center of Strategic & International Studies* (April 2005): 1.

Keohane Robert and Joseph Nye, Jr., Introduction, *Governance in a Globalizing World*, Washington : Brooking, 2000, hal. 26. dikutip dari Steven E. Bilet, Ph.D dalam *Transnational Advocacy and the Cyber Crime Convention : A Concideratioan of Lobbying and Global Governance*, The George Washington University, 2002.

Ari Juliano Gema, 2000, *Cyber crime : Sebuah Fenomena di dunia Maya.* www.bisnisindonesia.com. diakses pada tanggal 25 Maret 2009.

Pitoyo, Arif. "*Perlunya Penyempurnaan Hukum Pidana Tangani Cybercrime.*" http://gerbang.jabar.go.id/gerbang/index.php?index=16&idberita680, diakses pada tanggal 29 Agustus 2009.

Weimann, Gabriel. "*Cyberterrorism : How Real Is the Threat?,*" *USIP Special Report No. 119* (December 2004). http://www.usip.org/pubs/specialreports/sr119.html, diakses pada tanggal 29 Agustus 2009

Weimann, Gabriel, www.terror.net : *How Modern Terrorism Uses the Internet,* http://www.usip.org/pubs/specialreports/sr116.pdf, diakses pada tanggal 30 Agustus 2009.

Indra Safitri, "Tindak Pidana di Dunia Cyber". *Insider, Legal Journal From Indonesian Capital & Investmen Market,* http://business.fortunecity.com/buffett/842/art180199_tindakpidana.htm, diakses pada tanggal 20 Agustus 2009

Majalah Gatra edisi Oktober 2004, *Judul : Cybercrime di era digital*, website : http://www.gatra.com/2004-10-13/ date access Maret 2009

Wikipedia, http://en.wikipedia.org/wiki/Cyber-terrorism, diakses pada tanggal 29 Agustus 2009.

Zhang,http://www.slais.ubc.ca/courses/libr500/04-05 wt1/www/X_Zhang/5ways.htm , diakses pada tanggal 30 Agustus 2009.

BisTek Warta Ekonomi No. 24 edisi Juli 2000, *Judul : jenis-jenis kejahatan komputer.*

----, *FBI Tangkap Mafia Cyber* , http://cybertech.cbn.net.id, , data akses 02 Maret 2009.

----, *Data Pemilu KPU Diserang "Hacker"* , www.kompas.com, 08 Juli 2004.

----, "*Kejahatan Transnasional*", Http://www.YadeSetiawanUjung.com, diakses pada tanggal 26 Agustus 2009

----, "*Federal Bureau of Investigation (FBI), citation Adam Savino, CyberTerrorisme*", http://www.cybercrimes.net/Terrorism/ct.html, diakses pada tanggal 28 Agustus 2009.

----, "*Electronic Civil Defence*", http://ntrg.cs.tcd.ie/undergrad/4ba2.02/infowar/ecd.html, diakses pada tanggal 29 Agustus 2009

http://www.suaramerdeka.com/harian/0207/24/nas13.htm. diakses pada tanggal 25 Agustus 2009

http://cybercrime.wordpress.com/, diakses pada tanggal 25 Agustus 2009

http://www.duniamaya.org/index.php/security/kejahatan-dunia-maya-cybercrime/, diakses pada tanggal 25 Agustus 2009

http://www.pikiran-rakyat.com, diakses pada tanggal 17 September 2009.

Http://www.asphost.com/cyber_crime/contohkasus.html diakses pada tanggal 28 Oktober 2009