Karya Ilmiah

PENANGGULANGAN KEJAHATAN INTERNASIONAL CYBER CRIME DI INDONESIA

Oleh : Dr. H. Obsatar Sinaga, M.Si

Dosen Pasca Sarjana Universitas Padjadjaran Bandung

MAKALAH

Bahan Diskusi Seminar Nasional

Ikatan Cendikiawan Muslim se-Indonesia (ICMI)

AULA ICC IPB BOGOR, 5 Desember 2010

DAFTAR ISI

PENDAHULUAN

Latar Belakang

Saat ini, teknologi informasi dan komunikasi mengalami perkembangan yang sangat pesat, baik di Indonesia mau pun di seluruh dunia. Hal ini ditandai dengan munculnya berbagai bentuk inovasi teknologi yang salah satunya adalah internet atau *interconnected network*. Internet merupakan teknologi digital hasil dari konvergensi antara teknologi telekomunikasi, media dan informasi. Keberadaan internet ini dimanfaatkan oleh masyarakat dunia dari berbagai kalangan untuk berbagai kegiatan, seperti mencari informasi, mengirim informasi dan melakukan kegiatan bisnis atau non bisnis. Kegiatan ini dikenal sebagai kegiatan telematika (*cyber activities*). Di dalam *cyber activities* peran teknologi sangat besar, karena semakin tinggi teknologi yang dimiliki maka semakin besar pula peluang masyarakat untuk menggunakan internet dalam kehidupan sehari-hari. Pengguna internet ini terbagi menjadi pengguna pasif dan aktif. Pengguna pasif adalah para pengguna yang hanya membuka *web pages* di internet (*browsing*) atau membaca informasi tanpa melakukan interaksi baik dengan *vendor/administrator* atau pengguna internet lainnya. Pengguna internet aktif adalah para pengguna yang melakukan interaksi dengan *vendor* atau dengan pengguna internet lainnya, contohnya, berbelanja secara *online*, mengirim surat elektronik (e-mail) dan lain sebagainya. Pengguna aktif ini juga dapat menggunakan media internet untuk melakukan tindakan yang dikategorikan sebagai kejahatan telematika (*cyber crime*). Kejahatan telematika adalah tindakan kejahatan yang dilakukan dengan menggunakan media internet. Contohnya, tindakan yang disebut *carding*, adalah *cyber crime* dengan cara mencuri data kartu kredit dari nasabah suatu bank, sehingga si pelaku *carding (carder)* dapat menggunakan data tersebut untuk keuntungan pribadi.

Kejahatan lain seperti yang muncul di Indonesia belum lama ini adalah 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 teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.[1]

Kejahatan telematika sangat menggunakan komputer baik sebagai alat untuk mencapai tujuan dari kejahatan tersebut (*computer as a tool*) mau pun komputer sebagai target kejahatan (*computer as a target*). Pada dasarnya originalitas kejahatan telematika adalah kejahatan dimana komputer sebagai target, contohnya penyebaran virus atau *malicious ware*, sementara kejahatan dimana komputer sebagai alat adalah kejahatan tradisional yang menggunakan komputer sebagai sarana (contohnya *fraud* atau penipuan yang menggunakan *electronic mail* sebagai alat penyebaran informasi bagi si penipu). Kerugian yang timbul akibat adanya kejahatan telematika ini dari tahun ke tahun semakin meningkat. Berdasarkan data dari *The International Data Corporation* dan FBI, kerugian yang diderita Amerika atas kejatahan telematika ini meningkat dari US$ 2 Milliar pada tahun 1997 menjadi US$ 7.4 Milliar pada tahun 2003.[2] Kerugian atas kejahatan ini akan terus meningkat dua kali lipat setiap tahunnya, apabila tidak segera diantisipasi. Kejahatan telematika termasuk kejahatan yang bersifat lintas batas wilayah territorial suatu negara, karena jaringan (*network*) ICT yang digunakan termasuk sebagai jaringan yang tanpa batas (*borderless*). Jaringan *borderless* merupakan jaringan yang disediakan untuk memudahkan pengguna internet agar dapat mengakses informasi seluasluasnya, akan tetapi jaringan *borderless* dapat juga menimbulkan banyak permasalahan termasuk masalah kejahatan telematika yang sifatnya lintas batas wilayah Negara. Beberapa negara mengkategorikan kejahatan telematika sebagai kejahatan transnasional, sehinggga perlu adanya suatu kerjasama internasional dalam menangani kejahatan telematika tersebut. Akan tetapi banyak negara yang masih mengalami berbagai kesulitan dalam melaksanakan usaha baik pencegahan atau pun penanganan kejahatan telematika tersebut karena adanya ketidakseragaman dalam membuat regulasi dan aturan internal dalam negeri.

[1] www.usdoj.gov/criminal/cybercrimes
[2] Richard Power, ed., 2000, "2000 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends* 6, hlm. 3

Identifikasi Masalah

Cybercrime atau biasa disebut kejahatan telematika sudah tidak asing ditelinga masyarakat kita. Cybercrime seringkali dihubungkan dengan banyak kasus seperti kasus pembobolan ATM di beberapa bank di Indonesia, masalah terorisme, bahkan sampai kepada kasus pornografi. Banyak hal yang melatar belakangi kasus-kasus tersebut serta banyak hal pula yang mengancam stabilitas keamanan internasional. Dengan kata lain, ada kasus pasti harus ada penyelesaiannya. Dalam makalah ini, penulis juga akan menguraikan siapa saja yang aktor terlibat dalam kasus-kasus tersebut, siapa saja yang harus berperan dalam menanggulangi masalah cybercrime, dan peraturan perundang-undangan seperti apa yang diterapkan di beberapa negara seperti Amerika Serikat dan juga di Indonesia.

Makalah ini hanya akan membahas beberapa hal di bawah ini

1. Bagaimanakah sifat kejahatan telematika sebagai kejahatan transnasional?
2. Bagaimanakah pendekatan prinsip-prinsip yurisdiksi dalam hukum internasional dalam mengantisipasi dan menangani kejahatan telematika sebagai kejahatan transnasional?
3. Dengan cara bagaimana masyarakat internasional dapat mengantisipasi dan menangani kejahatan telematika tersebut?

Metode Kajian

Metode kajian yang digunakan penulis dengan *library research*, yaitu dengan mencari data-data via internet dan buku-buku terkait dengan masalah cybercrime dan hukum internasional.

PEMBAHASAN

Definisi Kejahatan Transnasional

Secara konseptual, transnational crime atau kejahatan transnasional adalah tindak pidana atau kejahatan yang melintasi batas negara. Konsep ini diperkenalkan pertama kali secara internasional di tahun 1990-an dalam The Eigth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.[3] Sebelumnya isitilah yang telah lebih dulu berkembang adalah *organized crime*. PBB sendiri menyebut *organized crime* sebagai *the large-scale and complex criminal activity carried on by groups of persons, however loosely or tightly organized, for the enrichment of those participating and at the expense of the community and its members*.[4] Pada perkembangannya PBB menambahakan bahwa istilan ini seringkali diartikan sebagai *the large-scale and complex criminal activities carried out by tightly or loosely organized associations and aimed at the establishment, supply and exploitation of illegal markets at the expense of society*.[5]

Menurut Mueller dalam Transnational crime: De¿nitions and Concepts, pada pertengahan tahun 1990-an, banyak peneliti mendefinisikan "kejahatan transnasional" untuk menyebut offences whose inception, prevention, and/or direct or indirect effects involve more than one country.[6] Mueller sendiri menggunakan istilah kejahatan transnasional untuk mengidentifikasi *certain criminal phenomena transcending international borders, trans-gressing the laws of several states or having an impact on another country*.[7]

---

[3] John R. Wagley, Transnational Organized Crime:Principal Threats and U.S. Responses (Congressional Research Service, The Library of Congress, 2006).
[4] United Nations, Changes in Forms and Dimensions of Criminality - Transnational and National, Working paper prepared by the Secretariat for the Fifth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Toronto, Canada, 1-12 September 1975).
[5] United Nations, Eigth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba 27 August to 7 September 1990, A/Conf.144/7, 26 July 1990.
[6] Gerhard O. W. Mueller, "Transnational Crime: Definitions and Concepts," Transnational Organized Crime 4, no. 1998 (n.d.).
[7] Ibid.

Menurut United Nations Convention on Transnational Organized Crime tahun 2000, kejahatan dapat dikatakan bersifat transnasional jika terdiri dari:[8]

1. dilakukan di lebih dari satu negara,

2. persiapan, perencanaan, pengarahan dan pengawasan dilakukan di negara lain,

3. melibatkan organized criminal group dimana kejahatan dilakukan di lebih satu negara, dan

4. berdampak serius pada negara lain.

Kejahatan transnasional merupakan fenomena sosial yang melibatkan orang, tempat dan kelompok, yang juga dipengaruhi oleh berbagai sosial, budaya, faktor ekonomi.[9] Akibatnya, berbagai negara cenderung memiliki definisi kejahatan transnasional yang sangat berbeda tergantung pada filosofi tertentu. Menurut Martin dan Romano, *transnational crime may be defined as the behavior of ongoing organizations that involves two or more nations, with such behavior being defined as criminal by at least one of these nations.*[10]

Berdasarkan beberapa uraian diatas, menurut saya kejahatan transnasional merupakan kejahatan yang terjadi antar lintas negara yang dapat dikategorikan sebagai kejahatan yang terorganisasi dengan baik dan penuh dengan perencanaan matang. Dalam setiap peristiwa kejahatan transnasional aktornya tidak selalu berkaitan dengan nation-state actor, melainkan individu, dan kelompok. Dalam setiap aksinya para mereka tidak hanya berperan sebagai pelaku tetapi juga sebagai penyumbang dana maupun pikiran untuk melancarkan aksinya. Latar belakang kejahatan ini juga cukup luas, menyangkut bidang politik, ekonomi, sosial, budaya, agama, dll. Bannyak juga kejahatan transnasional yang tidak terkait dengan latar belakang tersebut.

[8] Muladi, Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia, 1st ed. (Jakarta: The Habibie Center, 2002).
[9] Mark Findlay, The globalization of Crime: Understanding Transnational Relationship in Context (Cambridge University Press, 2003).
[10] Martin, J. M. and Romano, A. T., Multinational Crime-Terrorism, Espionage, Drug & Arms Trafficking (SAGE Publications, 1992

Suatu kejahatan dapat dikategorikan sebagai kejahatan transnasional atau bukan dapat dilihat dari:

1. melintasi batas negara,
2. pelaku lebih dari satu, bisa nation-state actor ataupun yang lain,
3. memiliki efek terhadap negara ataupun aktor internasional (misalnya individu ±dalam pandangan kosmopolitan) di negara lain,
4. melanggar hukum di lebih dari satu negara,

Pada tahun 1995, PBB telah mengidentifikasi 18 jenis kejahatan transnasional, yaitu pencucian uang, terorisme, pencurian benda seni dan budaya, pencurian kekayaan intelektual, perdagangan senjata gelap, pembajakan pesawat, pembajakan laut, penipuan asuransi, kejahatan komputer, kejahatan lingkungan, perdagangan orang, perdagangan bagian tubuh manusia, perdagangan narkoba, penipuan kepailitan, infiltrasi bisnis, korupsi, dan penyuapan pejabat publik atau pihak tertentu.[11]

PBB mengidentifikasi jenis-jenis kejahatan yang melintasi batas negara dan pelaku lebih dari satu memiliki efek terhadap aktor di negara lain melanggar hukum di lebih dari satu negara seperti, pencucian uang, terorisme, pencurian benda seni dan budaya, pencurian kekayaan intelektual, perdagangan senjata gelap, pembajakan pesawat, pembajakan tanah, serta pembajakan laut.[12]

Definisi Cyber Crime (Kejahatan Telematika)

Cyber crime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Beberapa pendapat mengindentikkan cyber crime dengan computer crime. The U.S. Department of Justice memberikan pengertien computer crime sebagai:

[11] Garda T. Paripurna, Sekilas Tentang Kejahatan Transnasional, Riset Hukum Kejahatan Transnasional, 2008,
[12] www.scribd.com/doc/.../Definisi-Transnational-Crime

"…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution".[13]

Dalam tulisannya Andi Hamzah (1989) berkata bahwa, "Aspek-aspek Pidana di Bidang komputer", mengartikan kejahatan komputer sebagai:

"Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal".

Definisi tersebut identik dengan yang diberikan Organization of European Community Development, yang mendefinisikan *computer crime* sebagai:

"any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data".

Dari beberapa definisi di atas, secara singkat dapat saya katakan bahwa *cybercrime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet sebagai media utama yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. Dalam kasus ini tentunya kita akan sulit melacak untuk menemukan siapa orang yang melakukan kejahatan tersebut, tetapi bukan tidak mungkin pelakunya dapat ditemukan.

Kejahatan Telematika sebagai Kejahatan Transnasional

Kejahatan transnasional adalah kejahatan yang tidak hanya sifatnya lintas batasNegara, tetapi termasuk juga kejahatan yang dilakukan di suatu Negara, tetapi berakibat fatal bagi Negara lain. Contoh kejahatan transnasional ini adalah *human trafficking*, penyelundupan orang, narkotika, atau teroris internasional.

Saat ini, beberapa Negara mengkategorikan kejahatan telematika sebagai kejahatan transnasional, karena tindakannya bisa dilakukan di Negara B, oleh warga Negara A, tetapi korbannya ada di Negara C. Dalam tatanan teknologi, sifat kegiatan telematika adalah *borderless* atau lintas batas negara. Dimensi transnasional yang melekat pada teknologi telematika ini

[13] www.usdoj.gov/criminal/cybercrimes

sangat menguntungkan pelaku kejahatan. Pelaku kejahatan dapat melakukan kejahatannya pada korban di negara manapun korban berada. Korban kejahatan telematika tidak terbatas pada individu, tetapi juga organisasi atau perusahaan bahkan negara secara keseluruhan. Keuntungan yang lain bagi pelaku kejahatan telematika adalah disparitas aturan berkaitan dengan kejahatan telematika di setiap negara. Bahkan masih banyak negara yang belum memiliki hukum yang mengatur khusus mengenai kejahatan telematika. Hal ini tentu memudahkan pelaku kejahatan telematika bisa dengan leluasa melakukan aktifitasnya tanpa terjerat hukum. Terdapat beragam contoh kasus mengenai kejahatan telematika sebagai kejahatan transnasional.

Karakteristik Cyber Crime[14]

Berdasarkan motif kegiatannya, kejahatan telematika (cyber crime) dapat digolongkan kedalam:

a. Kejahatan kerah biru (*blue collar crime*)

   Kejahatan ini merupakan jenis kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti misalnya perampokkan, pencurian, pembunuhan dan lain-lain.

b. Kejahatan kerah putih (*white collar crime*)

   Kejahatan jenis ini terbagi dalam empat kelompok kejahatan, yakni kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu.

Cybercrime 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 berikut:

1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Pelaku kejahatan

[14] irmarr.staff.gunadarma.ac.id/.../files/.../Modus+Kejahatan+dalam+TI.doc

4. Modus Kejahatan

5. Jenis kerugian yang ditimbulkan

Jenis Cybercrime[15]

Berdasarkan jenis aktifitas yang dilakukannya, cybercrime dapat digolongkan menjadi beberapa jenis sebagai berikut:

1. *Unauthorized Access*

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. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi Internet/intranet. Kita tentu belum lupa ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa *website* milik pemerintah RI dirusak oleh *hacker* (Kompas, 11/08/1999). Beberapa waktu lalu, *hacker* juga telah berhasil menembus masuk ke dalam *data base* berisi data para pengguna jasa America Online (AOL), sebuah perusahaan Amerika Serikat yang bergerak dibidang *ecommerce* yang memiliki tingkat kerahasiaan tinggi (Indonesian Observer, 26/06/2000). Situs Federal Bureau of Investigation (FBI) juga tidak luput dari serangan para *hacker*, yang mengakibatkan tidak berfungsinya situs ini beberapa waktu lamanya untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan computer (*computer network system*) pihak asaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (*data base*) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer).[16]

[15] laluilmi.blogspot.com/.../modus-modus-kejahatan-dalam-it.html
[16]

2. *Illegal Contents*

kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum. Contoh rilnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya, seperti penyebaran pornografi.

3. Penyebaran virus secara sengaja

Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

4. *Data Forgery*

Kejahatan yang 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. Kejahatan ini biasanyaditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

5. *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.

6. *Cyberstalking*

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer.

7. *Carding*

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

8. *Hacking and 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.

9. *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.

10. *Hijacking*

Merupakan kejahatan melakukan pembajakan hasil karya orang lain.

11. *Cyber Terorism*

Suatu tindakan *cybercrime* 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 DoktorNuker diketahui telah kurang lebih lima tahun melakukan defacing atau mengubah isi halaman web dengan propaganda anti-American, anti-Israel dan pro-Bin Laden.

Macam-Macam *Cyber Crime* Berdasarkan Sasaran Kejahatannya

1. Kejahatan telematika terhadap individu[17]

Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain :

- Pornografi

Kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas.

- *Cyberstalking*

Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia cyber. Gangguan tersebut bisa saja berbau seksual, religius, dan lain sebagainya.

- *Cyber-Tresspass*

Kegiatan yang dilakukan melanggar area privasi orang lain seperti misalnya Web Hacking. Breaking ke PC, Probing, Port Scanning dan lain sebagainya.

Contoh kasus lainnya adalah lima orang hacker (penyusup) yang berada di Moskow telah mencuri sekitar 5400 data kartu kredit milik orang Rusia dan orang asing yang didapat dengan menyusup pada sistem komputer beberapa *internet retailer*, terhitung dari tahun 1999 sampai

[17] irmarr.staff.gunadarma.ac.id/.../files/.../Modus+Kejahatan+dalam+TI.doc

dengan April 2000. Kerugian yang diderita ditaksir sebesar US$ 630.000.[18] Kejahatan ini dapat ditangani oleh Pemerintah Rusia, dengan menjatuhkan hukuman pencurian pada kelima orang carder tersebut. Akan tetapi kerugian yang diderita para korban sampai saat ini belum ditangani.

2. Cybercrime menyerang hak milik (*Againts Property)*

Cybercrime yang dilakukan untuk menggangu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia cyber, pemilikan informasi elektronik secara tidak sah/pencurian informasi, carding, cybersquating, hijacking, data forgery dan segala kegiatan yang bersifat merugikan hak milik orang lain.

3. Kejahatan telematika terhadap perusahaan atau organisasi

Pada tahun 1995, Julio Cesar Ardita, seorang mahasiswa dari Argentina berhasil menyusup dan mengganti (*cracking*) data sistem yang ada di Fakultas *Arts and Science* Universitas Harvard, Departemen Pertahanan Amerika, *the US Naval Command, the San Diego-based Control and Ocean Surveillance Center*, dan beberapa organisasi vital di Amerika. Sayangnya, Hukum Argentina tidak mengatur tindakan Ardita sebagai kejahatan. Meskipun begitu, mengingat kerugian yang diderita oleh Pemerintah Amerika, pada akhirnya Julio Cesar Ardita menyerahkan diri dengan sukarela kepada FBI.[19]

4. Kejahatan telematika terhadap negara

Majalah New York Times melaporkan sering kali terjadi serangan terhadap situssitus resmi di beberapa Negara di dunia, yang dilakukan bahkan bukan oleh warga Negaranya. Serangan yang paling merugikan adalah pengrusakan yang dilakukan oleh hacker asing pada situs Kementrian keuangan Romania pada tahun 1999, sehingga merugikan pemerintah Romania milyaran dollar. Serangan ini dilakukan dengan mengganti besaran kurs mata uang Romania sehingga banyak pembayar pajak online yang terkecoh dengan data yang telah diganti tersebut.[20]

---

[18] Suspected Russia Hackers Held," New York Times on the Web/Breaking News from Associated Press, April 28, 2000, reported at _http://www.nytimes.com/ aponline/i/AP-Russia-Hackers.html_.

[19] David Berlind, "Reno's Border Patrol Made Ineffective," PC Week, April 8, 1996, hlm. 78.

[20] See "Hackers Alter Romanian Money Rate," New York Times on the Web/ Breaking News from

Hanya sayangnya, kejahatan ini tidak berlanjut ke pengadilan karena tidak adanya hukum yang mengatur kejahatan telematika yang bersifat transnasional.

Kejahatan telematika yang merugikan banyak negara adalah kasus "Virus Melissa". Virus ini dibuat oleh David L. Smith, seorang programmer dari New Jersey. Dia menciptakan virus Melissa dan menggunakan situs X-rated untuk menyebarkan virus tersebut atau melalui e-mail. Virus ini tidak bisa dijinakan sehingga merugikan banyak perusahaan-perusahaan di dunia dengan perkiraan kerugian sebesar US$ 80 milyar. Untuk kejahatannya ini Smith dijatuhi hukuman penjara 5 tahun oleh Pengadilan Negara Bagian New Jersey.[21]

Bagi Amerika, kejahatan telematika sudah menjadi agenda penting dalam peraturan perundang-undangan negara tersebut, sehingga sejak tahun 1997, Amerika terus memperbaharui hukum mengenai kejahatan telematika. Akan tetapi bagi Negara-negara lain, terutama Negara berkembang yang sering menjadi lahan kejahatan telematika, sulit untuk mengadili pelaku kejahatan tersebut, terutama apabila kejahatan itu dilakukan bukan oleh warga negaranya dan dilakukan tidak didalam wilayah teritorialnya, meskipun Negara tersebut mengalami kerugian. Hal ini yang mendorong beberapa negara melakukan berbagai upaya untuk membuat aturan mengenai tindakan pencegahan dan penanganan kejahatan telematika, akan tetapi efektifitas aturan tersebut bergantung pada masing-masing negara. Misalnya, pada tanggal 4 Desember 2000, Sidang Umum Perserikatan Bangsa-Bangsa (PBB) telah menandatangani Resolusi PBB 55/63 mengenai anjuran bagi negara-negara anggota PBB untuk memerangi tindakan kejahatan telematika atau tindakan penyalahgunaan teknologi informasi. Menindaklanjuti Resolusi PBB 55/63, para pemimpin ekonomi yang tergabung dalam organisasi Kerja Sama Ekonomi Asia Pasifik (APEC) sepakat membentuk APEC *Cyber Crime Strategy* yang bertujuan mengupayakan secara bersama keamanan internet (*cyber security*) dan mencegah serta menghukum pelaku kejahatan telematika. Sementara itu, Negara-negara anggota ASEAN sepakat membentuk *Manila Declaration on Prevention and Control of Transnational Crime,* yaitu deklarasi mengenai pencegahan dan pengawasan kejahatan transnasional termasuk kejahatan yang

---

Associated Press, November 3, 1999, reported at _http:// www.nytimes.com/aponline/i/AP-Romania-Hackers.html_.

[21] "Melissa Virus Exposes Computer Users' Vulnerability," *Japan Computer Industry Scan*, April 12, 1999, available at 1999 WL 9642279;

menggunakan ICT atau kejahatan telematika. Akan tetapi upaya masayarakat internasional tersebut di atas hanya sebatas *morally and political binding* bagi negara-negara anggota, sehingga pelaksanaannya diserahkan atas dasar kemauan dan kemampuan negara-negara tersebut. Lain halnya dengan Eropa dimana negara-negara yang tergabung dalam European Union telah membentuk *International Convention on Cyber Crime* pada tahun 2001, dan efektif dilaksanakan pada pertengahan tahun 2004. Konvensi ini mengikat negara-negara eropa union yang meratifikasinya, sehingga kejahatan telematika yang terjadi di wilayah eropa dapat ditangani secara regional. Namun timbul pertanyaan yang mendasar, bagaimana Negara-negara tersebut melakukan penanganan kejahatan telematika yang bersifat transnasional? Berkaitan dengan ketentuan mengenai yurisdiksi Negara. Hal yang penting adalah bagaimana pendekatan yurisdiksi negara terhadap kejahatan telematika yang bersifat transnasional. Yurisdiksi secara konseptual dibagi menjadi tiga yaitu:[22]

- Jurisdiction To Prescribe

Negara berwenang menetapkan ketentuan hukum baik pidana ataupun perdata pada subjek hukum atau peristiwa hokum yang terjadi diwilayahnya atau yang dilakukan oleh warga negaranya.

- Jurisdiction To Adjudicate

Negara berwenang untuk memaksa subjek hukum untuk tunduk pada proses peradilan, baik proses pidana maupun perdata

- Jurisdiction To Enforce

Negara berwenang untuk memaksa subjek hukum untuk memenuhi kewajibannya, atau melaksanakan hukuman yang telah diputuskan oleh badan peradilan negara tersebut. Pada dasarnya ketiga konsep ini termasuk dalam prinsip yurisdiksi territorial, dimana satu Negara memiliki kewenangan dalam menetapkan hokum pidananya terhadap kejahatan yang berlangsung didalam wilayah teritorialnya. Ketentuan mengenai apakah bentuk kegiatan tersebut dapat dipidana tergantung dari hokum Negara dimana tindakan tersebut dilakukan. Hal ini terjadi

[22] vub.academia.edu/.../KEJHATAN_TELEMATIKA_SEBAGAI_KEJAHATAN_TRANSNASIONAL.pdf

pada tahun 2000, kasus virus ,“I love You“ yang merugikan sekitar 40 juta orang di Amerika, menimbulkan permasalahan yurisdiksi. Virus yang dibuat oleh Guzman warga negara Philipina tidak dianggap sebagai kejahatan berdasarkan hukum Philipina, sebaliknya Amerika menetapkan Guzman sebagai penjahat cyber yang harus ditindak dan diadili. Kenyataan ini menggambarkan bahwa, kejahatan telematika yang bersifat transnasional membutuhkan adannya pengakuan „“double criminality“, yaitu baik Amerika maupun Philipina sama – sama mengakui bahwa penyebaran virus termasuk sebagai kejahatan. Sehingga dimungkinkan adanya ekstradisi, atau paling tidak adanya *legal mutual assistance*, dimana kejahatan itu dilaporkan oleh pihak Amerika, sedangkan penangannya dapat dilakukan oleh Philipina.

Kasus lain adalah Yahoo.com Inc. yang dilarang didownload di wilayah Jerman dan Inggris pada tahun 2004-2005. Hal ini dikarekan Yahoocom dan America Online.Com menampilkan memoribilia Nazi. Pemerintah Jerman memerintahkan untuk mendenda setiap ISP yang menampilkan Yahoo.com tersebut. Hal ini tentu diprotes oleh Yahoo.inc, karena kegiatan uploading Nazi memoribilia ini tidak bertentangan dengan hukum Federal Amerika. Kasus lain terjadi antara Pemerintah Amerika dan Antigua, ketika pada tahun 2006, FBI meminta Interpol untuk mengeluarkan *'Red Notice'* untuk menangkap Presiden Perusahaan Gambling Online dari Antigua. Amerika menganggap bahwa gambling online yang berasal dari Antigua adalah melawan hukum Federal. Hanya saja, permintaan FBI untuk menangkap pelaku yang menyebarkan online gambling ditolak oleh Antigua karena kegiatan online gambling tersebut tidak bertentangan dengan hukum Antigua. Permasalahan yurisdiksi ini kemudian timbul ketika masing – masing negara mengklaim memiliki ketentuan yurisdiksi tersendiri dalam menangani kejahatan telematika. Beberapa prinsip yang mendasari klaim tersebut adalah :

Prinsip Territorial Claims[23]

Pada prinsip teritorial klaim ini negara-negara memiliki ketentuan hukumnya berdasarkan:

1. Lokasi dimana kejahatan telematika dilakukan

[23] vub.academia.edu/.../KEJHATAN_TELEMATIKA_SEBAGAI_KEJAHATAN_TRANSNASIONAL.pdf

Dalam Konvensi *Cyber Crime* pada Pasal 2 sampai Pasal 11 menyatakan, bahwa setiap peserta konvensi berhak menetapkan yursidiksinya terhadap setiap kejahatan telematika yang dilakukan didalam wilayah teritorialnya. Contohnya, apabila X seseorang dari Jerman mengirim virus melalui E-Mail kepada Y seseorang yang berada di Indonesia, kemudian Y menyebarkan virus tersebut di Indonesia, maka X dapat dikenai pidana berdasarkan hukum Jerman. Hanya saja ketentuan ini akan sulit dibuktikan terutama apabila tidak adanya klaim dari pihak yang dirugikan.

2. Lokasi dimana komputer sebagai alat kejahatan berada

Pada hukum telematika Singapura terdapat ketentuan mengenai apabila computer sebagai media kejahatan telematika berada didalam yurisdiksi Singapura, maka pemerintah Singapura memiliki kewenangan untuk menangkap dan mengadili pelakunya, meskipun pelakunya adalah bukan warga negara Singapura. Mengingat bahwa akibat dari kejahatan tersebut bisa berdampak baik pada warga singapura atau pun diluar Singapura. Contohnya kasus Danny, seorang pelajar Indonesia yang diadili di Singapura karena melakukan *hacking* pada beberapa situs baik situs Singapura atau situs dari luar singapura, akan tetapi tindakannya dilakukan di Singapura.

3. Lokasi Korban Kejahatan Telematika

Lokasi korban kejahatan telematika ini menjadi hal yang krusial yang ada pada yurisdiksi kejahatan telematika. Pada kejahatan *Child Phornography*, Negara A bisa mengklaim untuk menghukum pelaku *child phornography*, meski pelaku adalah warga negara B, apabila terbukti bahwa korban adalah anak-anak di negara A.

4. Prinsip *Personality Claims*

Setelah prinsip teritorial klaims, *Personality Claims* merupakan prinsip berikutnya dalam yurisdiksi kejahatan telematika. Dalam Konvensi Cyber Crime, diatur mengenai personality claim bagi pelaku kejahatan telematika. Pasal 22 Konvensi mengatur bahwa *"The Cybercrime Convention requires parties to establish jurisdiction "when the offence is committed (. . .) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State."* Hanya saja di masing-masing Negara peserta Konvensi Cyber Crime memiliki interpretasi yang berbeda. Jerman

memiliki ketentuan mengenai pemidanaan bagi warga Negara Jerman yang melakukan kejahatan telematika di luar wilayah Jerman, apabila tindakan tersebut juga dianggap sebagai kejahatan telematika oleh hukum Negara dimana kejahatan tersebut dilakukan. Contohnya, tindakan spy menggunakan keylogger di wilayah hukum Jerman adalah kejahatan telematika, akan tetapi Gaul seorang warga Negara Jerman melakukan tindakan tersebut di wilayah Fiji, yang notabene tidak mengatur bahwa tindakan Spy adalah kejahatan, sehingga Gaul tidak dapat dipidana. Akan tetapi, ketika seorang warga Jerman melakukan akses tanpa ijin pada system computer di Amerika, kemudian orang tersebut kembali ke Jerman, maka pemerintah Jerman dapat menangkap dan mengadili orang tersebut karena melakukan kejahatan telematika dan melanggar hukum federal tentang *cybercrime* di Amerika. Selain itu yurisdiksi kejahatan telematika mengenal personality claim dari sisi korban. Di Amerika, ketentuan hukum federal Amerika mengenai cyber crime yang diatur pada U.S. Code no. 1030 mengatur mengenai yurisdiksi untuk mengadili bagi siapa saja yang melakukan sabotase pada system computer milik pemerintah Amerika. Meskipun kejahatan tersebut dilakukan diluar wilayah Amerika. Hal ini serupa dengan ketentuan Pasal 37 Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elaktronik yaitu "Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia." Hanya permasalahannya selalu terbentur pada masalah extradisi, karena tidak semua Negara memiliki perjanjian ekstradisi yang berlaku bagi pelaku kejahatan telematika.

Dua Macam Prinsip Ekstradisi[24]

Prinsip Perlindungan

Konsep ini dapat diterapkan oleh setiap negara untuk melaksanakan yurisdiksi terhadap kejahatan yang menyangkut keamanan dan integritas atau kepentingan ekonominya. Prinsip ini dapat diterapkan terhadap warga negara asing yang melakukan kejahatan di luar wilayahnya tetapi diduga dapat mengancam kepentingan keamanan, integritas dan kemerdekaan negara

[24] vub.academia.edu/.../KEJHATAN_TELEMATIKA_SEBAGAI_KEJAHATAN_TRANSNASIONAL.pdf

tersebut. Contohnya, pada tahun 2004 seorang *Hacker* Amerika memainkan "wargames" dan menyelundup kedalam sistem keamanan nasional Inggris. Sistem keamanan Inggris ini digunakan untuk memeras pemerintah Inggris. Sehingga Pemerintah Inggris menuntut hacker tersebut untuk diekstradisi dan diadili di Inggris, akan tetapi pihak Amerika mengklaim bahwa Pemerintah Amerika yang berhak untuk menerapkan yurisdiksinya.

Prinsip Universal

Untuk beberapa kejahatan telematika tertentu seperti kejahatan *child phornography,* perdagangan anak dan perempuan lewat internet, terorisme (contohnya transfer dana untuk kegiatan terorisme melalui elektronik perbankan) dan jual beli narkotika melalui internet, maka banyak Negara yang mengklaim kejahatan tersebut dapat dipidana di negaranya berdasarkan prinsip universal. Dari paparan di atas, hal yang timbul menjadi pertanyaan adalah bagaimana Negara-negara di dunia menangani kejahatan telematika yang bersifat transnasional. Langkah-langkah yang dapat diambil adalah :

1. Adanya persamaan persepsi dari negara-negara mengenai bentuk kejahatan telematika apa saja yang dianggap sebagai kejahatan telematika yang bersifat transnasional.
2. Adanya kerjasama antar Negara berkaitan dengan alih teknologi dalam usaha melakukan penyelidikan dan penyidikan terhadap kejahatan telematika
3. Adanya kesamaan persepsi mengenai *digital evidence* pada hokum nasional setiap negara
4. Membentuk perjanjian internasional atau regional mengenai kejahatan telematika. Saat ini hanya Eropa yang memiliki Konvensi mengenai *cybercrime,* akan tetapi tidak menutup kemungkinan negara lain dapat meratifikasi konvensi tersebut.
5. Adanya perjanjian ekstradisi bagi pelaku kejahatan telematika atau setidaknya kerjasama *Mutual Legal Assistance*

Upaya Penanggulangan Cybercrime[25]

Aktivitas pokok dari cybercrime adalah penyerangan terhadap *content, computer system* dan *communication system* milik orang lain atau umum di dalam *cyberspace*. Fenomena cybercrime memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan. Berikut ini cara penanggulangannya :

Mengamankan sistem

Tujuan yang nyata dari sebuah sistem keamanan adalah mencegah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem secara terintegrasi sangat diperlukan untuk meminimalisasikan kemungkinan perusakan tersebut. Membangun sebuah keamanan sistem harus merupakan langkah-langkah yang terintegrasi pada keseluruhan subsistemnya, dengan tujuan dapat mempersempit atau bahkan menutup adanya celah-celah *unauthorized actions* yang merugikan. Pengamanan secara personal dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya menuju ke tahap pengamanan fisik dan pengamanan data. Pengaman akan adanya penyerangan sistem melalui jaringan juga dapat dilakukan dengan melakukan pengamanan FTP, SMTP, Telnet dan pengamanan *Web Server*.

Penanggulangan Global

The Organization for Economic Cooperation and Development (OECD) telah membuat guidelines bagi para pembuat kebijakan yang berhubungan dengan computer-related crime, dimana pada tahun 1986 OECD telah memublikasikan laporannya yang berjudul Computer-Related Crime : Analysis of Legal Policy. Menurut OECD, beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime adalah :

1. melakukan modernisasi hukum pidana nasional beserta hukum acaranya.

[25] irmarr.staff.gunadarma.ac.id/.../files/.../Modus+Kejahatan+dalam+TI.doc

2. meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.

3. meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*

4. meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya mencegah kejahatan tersebut terjadi.

5. meningkatkan kerjasama antarnegara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cybercrime*.

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 cybercrime salah satunya. Cyber Crime merupakan bentuk perkembangan kejahatan transnasional yang cukup menghawatirkan saat ini.

Menurut Ahmad M. Ramli dalam sebuah artikel yang ditulis oleh dumadia.wordpress.com, instrumen hukum internasional publik yang saat ini mendapat perhatian adalah konvensi tentang kejahatan wasantara (convention on Cyber Crime) 2001 yang digagas oleh Uni Eropa. Konvensi ini meskipun pada awalnya dibuat oleh negara regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diaksesi oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan mayantara.

Pada tanggal 23 November 2001 negara-negara yang tergantung dalam Uni Eropa telah membuat dan menyepakati *Convention on Cyber Crime* di Budapest, Hongaria. Hasil dari konvensi tersebut kemudian dimasukan kedalam *European Treaty Series* dengan nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal 5 negara termasuk diratifikasi oleh 3 negara anggota *Council of Europe*. Substansi konvensi mencakup area yang cukup luas, bahkan mencakup kebijakan kriminal yang bertujuan untuk melindungi masyarakat dari cyber crime, baik melalui undang-undang maupun kerjasama internasional. Adapun yang menjadi pertimbangan dari pembentukan konvensi ini antara lain sebagai berikut:

1. Bahwa masyarakat internasional menyadari perlunya kerjasama antar negara dan industri dalam memerangi kejahatan mayantara dan adanya kebutuhan untuk melindungi kepentingan yang sah di dalam suatu negara serta pengembangan teknologi informasi.

2. Konvensi saat ini diperlukan untuk meredam penyalahnaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Dengan demikian, perlu adanya kepastian hukum dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dicapai, dipercaya dan cepat.

3. Saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak asasi manusia (HAM) dan konvenan PBB 1996 tentang hak politik dan sipil yang memberikan perlindungan kebebasasn berpendapat seperti hal berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyabarkan informasi dan pendapat.

Konvensi ini telah disepakati oleh Uni Eropa sebagai konvensi yang terbuka untuk diakses oleh negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrumen hukum internasional dalam mengatasi kejahatan may antara, tanpa mengurangi kesempatan setiap individu untuk tetap mengembangkan kreativitasnya dalam mengembangkan teknologi informasi. Di samping kedua instrumen tersebut, masih ada beberapa instrumen internasional yang dapat dijadikan acuan dalam mengatur teknologi informasi. Di samping kedua instrumen tersebut, masih ada beberapa instrumen internasional yang dapat dijadikan acuan dalam mengatur teknologi informasi. Instrumen tersebut dibuat oleh berbagai organisasi internasional, misalnya the United Nations Commisions on International Organizations (WTO), World Trade Organizations (WTO), dan sebagainya. Berikut ini akan diuraikan secara singkat tentang peraturan atau model law yang dikeluarkan oleh beberapa organisasi tersebut, antara lain:[26]

1. UNCITRAL, merupakan salah satu organisasi internasional yang pertama kali mulai membahas mengenai perkembangan teknologi informasi dan dampaknya terhadap perniagaan elektronik. Hasil dari UNCITRAL berupa model law yang sifatnya tidak

[26] dumadia.wordpress.com/.../upaya-internasional-dalam-menghadapi-cyber-crime/

mengikat, namun menjadi acuan atau model bagi negara-negara untuk mengadopsi atau memberlakukannya dalam hukum nasional Adapun beberapa model law yang telah ditetapkan oleh UNCITRAL terkait dengan perkembangan teknologi informasi adalah:

- UNCITRAL Model Law On E-Commerce
- UNCITRAL Model law On E-Commerce
- UNCITRAL Model on Electronic Signature
- UNCITRAL Model Law On International Credit Transfer.

2. WTO, peranan WTO adalah untuk membantu dalam regulasi perdagangan. WTO pertama kali membahas persoalan e-commerce pada bulan mei 1998. Pada bulamn Juli 1999, 4 badan utama dari WTO telah mengeluarkan laporan pertama mengenai pengaruh (initial impact assessments). WTO bermaksud membebaskan perdagangan teknologi Informasi. Pada konferensi tingkat menteri WTO pertama di Singapura, pada Desember 1999, para negosiator telah mengadopsikan Deklarasi Ministerial pada perdagangan dan produk teknologi informasi (Ministerial Declaration on Trade in Information Technology Product atau ITA). ITA menyediakan untuk mereka yang bersangkutan dalam menunda pembubaran pajak terhadap produk informasi teknologi yang diliputi oleh perjanjian tanggal 1 Januari 2000.

3. APEC, telah menyusun blue print for Action on Electronic Commerce pada bulan November 1998 yang menekankan peranan pemerintah untuk mendukung dan memfasilitasi perkembangan dan kemajuan e-commerce dengan:

   - Menyediakan lingkungan yang efektif, termasuk aspek hukum dan regulasi yang transparan dan konsisten
   - Menyediakan lingkungan yang mendukung kepercayaan dan keyakinan di antara pelaku e-commerce
   - Mendukung fungsi efisiensi dri e-commerce secara internasional dengan tujuan untuk membentuk suatu kerangka domestic

- Mempercepat dan mendorong penggunaan media elektronik.

4. OECD, pertama kali dimulai menggarap masalah e-commerce pada tahun 1998 di Ottawa dengan mengumumkan Actions Plan for Electronics Commerce yang antaranya merencanakan untuk:

   - Membangun kepercayaan untuk pengguna dan konsumen
   - Menetapkan aturan dasar untuk tempat pasar digital
   - Memperbaiki infrastruktur informasi untuk perdagangan elektronik
   - Memaksimalkan keuntungan dari perdagangan elektronik.

Resolusi Kongres PBB VIII tahun 1990 tentang The Prevention of Crime and Treatment of Offenders di Havana mengajukan bebrapa kebijakan dalam upaya menaggulangi cyber crime, antara lain sebagai berikut:

1. Menghimbau negara anggota untuk menginvestasikan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah di antaranya.
2. Melakukan modernisasi hukum pidana material dan hukum acara pidana
3. Mengembangkan tindakan-tindakan pencegahan dan pengamanan computer
4. Melakukan langkah-langkah untuk membuat peka warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan computer
5. Melakukan upaya-upaya pelatihan (training) bagi para hakim, pejabat dan para penegak hukum mengenai kejahatan ekonomi dan cyber crime
6. Memperluas rules of ethics dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika

7. Mengadopsi kebijakan perlindungan korban Cyber Crime sesuai dengan deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk korban melaporkan adanya cyber crime.

8. Menghimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggualngan Cyber Crime.

9. Merekomendasikan kepada Komite Pengendalian dan Pencegahan Kejahatan (Committe on Crime Prevention and Control) PBB untuk:

   - Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi Cyber Crime di tingkat nasional, regional dan internasional.

   - Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem Cyber Crime pada masa yang akan datang.

   - Mempertimbangkan Cyber Crime sewaktu meninjau pengimplementasian perjanjian ekstradisi dan bantuan kerja asma di bidang penanggulangan kejahatan. Upaya internasional dalam penanggulangan cyber crime, juga telah dibahas secara khusus dalam suatu lokakarya yaitu workshop on crime related to computer networks yang diorganisasi oleh UNAFEI selama Kongres PBB X tahun 2000 berlangsung. Adapun kesimpulan dari lokakarya ini adalah sebagai berikut :

     a. Computer Related Crime (CRC) harus dikriminalisasikan.

     b. Diperlukan hukum acara yang tepat untuk penyidikan dan penuntutan terhadap penjahat mayantara (cyber criminals).

     c. Harus ada kerja antara pemerintah dan industri terhadap tujuan umum pencegahan dan penaggulanagn kejahatan komputer agar internet menjadi aman.

     d. Diperlukan kerjasama internasional untuk menelusuri atau mencari para penjahat internet.

     e. PBB harus mengambil langkah atau tindak lanjut yang berhubungan dengan bantuan dan kerja sama teknis dalam penaggulangan computer related crime (CRC).

Demikianlah beberapa upaya hukum internasional yang terkait dengan upaya pencegahan dan penanggulangan Cyber Crime. Upaya pencegahan dan penanggulangan kejahatan mayantara dilaksanakan oleh masyarakat internasional oleh karena kejahatan ini adalah merupakan salah satu kejahatan baru yang beraspek internasional dan global. Upaya hukum saat ini tidak hanya terbatas pada perangkat model law, tetapi juga terkait dengan penegakan hukum (*law inforcement).*

Perlunya Dukungan Lembaga Khusus

Lembaga-lembaga khusus, baik milik pemerintah maupun NGO (*Non Government Organization*), diperlukan sebagai upaya penanggulangan kejahatan di internet. Amerika Serikat memiliki komputer *Crime and Intellectual Property Section* (CCIPS) sebagai sebuah divisi khusus dari U.S. *Departement of Justice*. Institusi ini memberikan informasi tentang *cybercrime*, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan *cybercrime*. Indonesia sendiri sebenarnya sudah memiliki IDCERT (*Indonesia Computer Emergency Rensponse Team*). Unit ini merupakan *point of contac*t bagi orang untuk melaporkan masalah-masalah keamanan komputer.

***Cybercrime* di Indonesia**

Penegakan Hukum Terhadap *Cybercrime*

Perlu kita yakini bahwa perkembangan teknologi dan informasi akan memacu pertumbuhan jenis kejahatan tertentu, karena perkembangan teknologi dan informasi selalu diikuti dengan perkembangan kriminalitas. Oleh karena itu, hukum pidana harus mengikuti perkembangan kriminalitas sehingga diharapkan dapat memberi perlindungan dan rasa keadilan dalam masyarakat, serta hukum tidak ketinggalan zaman, bahkan hukum harus dapat mencegah dan mengatasi kejahatan yang bakal muncul (Bakat Purwanto, 1995:4). Hukum pidana sebagai bagian dari keseluruhan hukum pada prinsipnya mempunyai fungsi dan tugas sebagai alat untuk melindungi hak asasi setiap orang maupun kepentingan masyarakat dan negara agar tercapai

keseimbangan, ketertiban, ketenteraman dan keamanan dalam menjaga kehidupan masyarakat (Adenan, 1995:74). Pemanfaatan komputer oleh penjahat dapat digunakan untuk melakukan kejahatan seperti kasus pembobolan BNI New York, BRI Cabang Brigjen Katamso Yogya, BDN Cabang Bintaro Jaya, Bank Danamon Pusat, Bank Danamom Glodok Plaza, percobaan pembobolan Union Bank of Switzerland (UBS), kasus Mustika Ratu dan banyak kasus-kasus lainnya. Dari uraian kasus-kasus tersebut di atas, dapat diketahui bahwa kejahatan tersebut dilakukan dengan menggunakan peralatan komputer, telekomunikasi dan informasi, namun landasan hukum yang digunakan adalah KUH Pidana yang belum memasukkan aturan hukum dengan aspek teknologi baru. Untuk penegakan hukum terhadapat *cyber crime* maka ada beberapa tindakan yang dapat dilakukan, seperti membuat peraturan perundang-undagan baru atau menambah beberapa pasal dalam peraturan perundang-undagan yang telah ada dan menentukan yurisdiksinya (Saefullah Wiradipradja dan Danrivanto Budhijanto, 2002:91).[27]

Beberapa negara seperti Amerika Serikat dan Kanada pemanfaatan teknologi informasi telah diatur secara nasional yang kemudian disusul oleh negara-negara yang tergabung dalam Uni Eropa. Di Asia seperti Singapura, India dan Malaysia telah mengatur pula kegiatan-kegiatan di dunia maya ini. Amerika serikat selain melakukan penyesuaian (berupa amandemen) terhada undang-undang yang memiliki relevansi dengan teknologi informasi juga dilakukan penyusunan undang-undang baru. Sesuai dengan sistem hukum yang dianut oleh Amerika Serikat, Kanada, Inggris, Singapura, Malaysia, India yaitu sistem hukum Anglo-Saxon, maka pengaturan mengenai pemanfaatan teknologi informasi dilakukan secara sektoral dan rinci. Setiap undang-undang hanya dimaksudkan untuk mengatur satu kegiatan tertentu saja. Apabila ditinjau dari sudut penerapannya, memang nampak lebih praktis dan terukur, namun kadang-kadang muncul kendala untuk mensinergikan dengan undang-undang lain yang memiliki keterkaiatan. Bagi Indonesia, sesuai dengan sistem hukum yang berlaku (kontinental) kiranya lebih tepat bila pengaturan tetatang pemanfaatan teknologi informasi disusun dalam suatu undang-undang yang bersifat pokok, namun mencakup sebanyak mungkin permasalahan (*umbrella provisions*). Mernurut E. Saefullah Wiradipradja dan Danrivanto Budhijanto(2002:91) Indonesia perlu pengaturan atas kegiatankegiatan *cyber space* dilandasi oleh tiga pemikiran untama yaitu:

[27] www.ajrc-aceh.org/.../PENEGAKAN%20HUKUM%20TERHADAP%20CYBE

1. Adanya kepastian hukum bagi para pelaku kegiatan-kegiatan di *cyber space* mengingat belum terakomondasinya secara memadai dalam peraturan perundang-undangan yang telah ada.

2. Upaya untuk mengantisipasi implikasi-implikasi yang ditimbulkan akibat pemanfaatan teknologi informasi, dan

3. Adanya variable global yaitu perdagangan bebas dan pasar terbuka (WTO/GATT)

Berkaitan dengan bentuk pengaturan di dalam *cyber space*, dapat ditinjau dari dua pendekatan, yaitu apakah perlu menciptakan norma-norma baru dan peraturan-peraturan khusus untuk kegiatan/aktivitas di *cyber space* atau apakah cukup diterapkan model-model peraturan yang dikenal di dunia nyata (konvensional) saja. Apabila diterapkan begitu saja kedua pendekatan tadi, ternyata sulit sekali memberlakukan ketentuan-ketentuan yang berlaku dalam dunia nyata ke dalam dunia maya. Karena ada beberapa ketentuan hukum konvensional yang tidak dapat diterapkan atau sulit untuk diterapkan dalam kegiatan-kegiatan *cyber space*, seperti tentang alat bukti, tandatangan, tempat atau domisili para pihak dalam kontrak, pengertian di muka umum dalam kasus pornografi. Oleh karena itu diperlukan ketentuan-ketentuan khusus dalam beberapa hal tertentu yang bersifat spesifik yang berlaku di *cyber space*. Untuk mengupayakan peraturan perundang-undangan berkaitan dengan "*computerrelated offences*" menurut Andi Hamzah (1993:43) perlu dilakukanbeberapa langkah antara lain:

1. Penetapan perbuatan apa yang menjadi interest berbagai pihak;

2. Penelitian mengenai, apakah peraturan perundang-undangan yang berlaku dapat digunakan memproses kejahatan komputer dan siber;

3. Identifikasi penyalahgunaan komputer dan siber yang melanggar kepentingan masyarakat;

4. Identifikasi kepentingan masyarakat yang perlu dilindungi dalam kaitannya dengan penggunaan komputer, informasi dan telekomunikasi;

5. Identifikasi dampak penetapan peraturan terhadap aspek sosial dan ekonomi.

Andi Hamzah juga mengingatkan untuk tidak terjadi "*over criminalization*. Dalam rangka penegakan hukum terdapat perbedaan pendapat tentang perlu tidaknya membentuk peraturan perundang-undangan baru dengan merumuskan tindak/perbuatan pidana atau *cyber crime*. (Heru Soepraptomo, 2001:14). Sementara itu ada yang berpendapat perlunya dibuat ketentuan khusus seperti; Teuku M. Radie, J.E. Sahetapy, Mulya Lubis, Sudama Sastraanjoyo, yang pada pokoknya memberi alasan bahwa hukum pidana yang ada tidak siap menghadapi kejahatan komputer, untuk menghadapi *white collar crime*, tindak pidana komputer adalah pidana khusus oleh karena itu perlu hukum khusus (Yosef Ardi, 2000). Pada saat pembuatan undang-undang yang berkaitan dengan *cyber space* juga perlu diperhatikan mengenai kompetensi pengadilan dalam menangani perkara *cyber crime*. Mengenai yurisdiksi dalam kegiatan *cyber space* perlu diperhatikan sejauhmanakah suatu negara memberi kewenangan kepada pengadilan untuk mengadili pelaku tindak pidana dalam kegiatan *cyber space*, khususnya dalam pemanfaatan teknologi informasi. Menurut Darrel Munthe, yurisdiksi di *cyber space* membutuhkan prinsipprinsip yang jelas dari hukum internasional dan hanya melalui prinsip-prinsip dalam yurisdiksi hukum internasional negara-negara dapat dibebankan untuk mengadopsi pemecahan yang sama terhadap yurisdiksi *cyber space* (Ny. Tien S. Saefullah, 2002:101). Pendapat di atas, dapat ditafsirkan bahwa dengan diakuinya prinsipprinsip yurisdiksi yang berlaku dalam hukum internasional oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasama dalm rangka harmonisasi ketentuan-ketentuan untuk menanggulangi *cyber crime*.

Dalam penggunaan *cyber space*, beberapa masalah dalam pembuktian akan timbul misalnya system "*digital signature"* yang berkaitan dengan hukum yang ada. Banyak negara mensyaratkan bahwa suatu transaksi harus disertai dengan bukti tertulis, dengan pertimbangan untuk adanya kepastian hukum. Permasalahan yang akan terjadi bagaimana sebuah dokumen elektronik yang ditandatangani dengan "*digital signature*" dapatkah dikatagorikan sebagai bukti tertulis? Di Inggris, bukti tertulis haruslah berupa tulisan (*typing*), ketikan *(printing*), litografi *(lithographi*) fotografi, atau bukti-bukti yang mempergunakan cara-cara lain yang dapat memperlihatkan atau mengolah kata-kata dalam bentuk yang terlihat secara kasat mata. Definisi dari bukti tertulis itu sendiri sudah diperluas hingga mencakup juga telex, telegram atau cara-cara lain dalam telekomunikasi yang menyediakan rekaman dari perjanjian. Indonesia sendiri dalam

Pasal 26 A Undang-undang No. 20 Tahun 2001 tentang Pemberantasn Tindak Pidana Korupsi juga telah memperluas pengertian tentang alat yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) KUHAP.

Menurut saya, alam kasus-kasus diatas jelaslah bahwa Undang-undang yang ada saat ini belum cukup bisa mengurangi atau bahkan menuntaskan masalah cybercrime. Justru malah semakin hari kasus-kasus seperti diungkapkan diatas semakin marak. Hal ini disebabkan oleh kurang tegasnya Undang-Undang yang sudah ada dan seharusnya benar-benar diterapkan. Bahkan mungkin perlu menambah pasal-pasal lainnya yang dirasa perlu ditambahkan. Seperti di Indonesia, saya kira semua warga negara Indonesia belum tentu paham tentang hal-hal yang terkandung dalam pasa-pasal terkait dengan Undang-Undang cybercrime itu sendiri. Berbeda dengan di Amerika Serikat atau negara-negara Asia lainnya seperti India, Singapura dan Malaysia, mereka lebih rinci lagi dalam menangani masalah cybercrime yaitu dengan menerapkan hukum Anglo-Saxon seperti yang diuraikan diatas. Selanjutnya, Undang-Undang juga membutuhkan revisi, harus mengikuti perkembangan zaman agar peraturan perundangan tersebut masih dapat berfungsi dengan baik.

Upaya Penanggulangan di Indonesia Oleh POLRI

Dalam artikel yang ditulis oleh Kombes (Pol) Drs. Petrus Reinhard Golose, M.M, ia mengungkapkan bahwa terdapat beberapa Undang-Undang terkait dengan Cybercrime (kejahatan telematika) yang berlaku di Indonesia, antara lain:[28]

a. Kitab Undang Undang Hukum Pidana

Dalam upaya menangani kasus-kasus yang terjadi para penyidik melakukan analogi atau perumpamaan dan persamaaan terhadap pasal-pasal yang ada dalam KUHP. Pasal-pasal didalam KUHP biasanya digunakan lebih dari satu Pasal karena melibatkan beberapa perbuatan sekaligus pasal-pasal yang dapat dikenakan dalam KUHP pada *cybercrime* antara lain :

1) Pasal 362 KUHP yang dikenakan untuk kasus *carding* dimana pelaku mencuri nomor kartu kredit milik orang lain walaupun tidak secara fisik karena hanya nomor kartunya saja yang

[28] BULETIN HUKUM PERBANKAN DAN KEBANKSENTRALAN
Volume 4 Nomor 2, Agustus 2006

diambil dengan menggunakan *software card generator* di Internet untuk melakukan transaksi di *e-commerce*. Setelah dilakukan transaksi dan barang dikirimkan, kemudian penjual yang ingin mencairkan uangnya di bank ternyata ditolak karena pemilik kartu bukanlah orang yang melakukan transaksi.

2) Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan di salah satu *website* sehingga orang tertarik untuk membelinya lalu mengirimkan uang kepada pemasang iklan. Tetapi, pada kenyataannya, barang tersebut tidak ada. Hal tersebut diketahui setelah uang dikirimkan dan barang yang dipesankan tidak datang sehingga pembeli tersebut menjadi tertipu.

3) Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban.

4) Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan *email* kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan *email* ke suatu *mailing list* sehingga banyak orang mengetahui cerita tersebut.

5) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara *online* di Internet dengan penyelenggara dari Indonesia.

6) Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun *website* porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut diluar negri dimana pornografi yang menampilkan orangdewasa bukan merupakan hal yang ilegal.

7) Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang yang vulgar di Internet , misalnya kasus Sukma Ayu-Bjah.

8) Pasal 378 dan 262 KUHP dapat dikenakan pada kasus *carding*, karena pelaku melakukan penipuan seolah-olah ingin membeli suatu barang dan membayar dengan kartu kreditnya yang nomor kartu kreditnya merupakan curian.

9) Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain, seperti *website* atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya.

b. Undang-Undang No 19 Tahun 2002 tentang Hak Cipta.

Menurut Pasal 1 angka (8) Undang- Undang No 19 Tahun 2002 tentang Hak Cipta, program computer adalah sekumpulan intruksi yang diwujudkan dalam bentuk bahasa, kode, skema ataupun bentuk lain yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi-fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang intruksi-intruksi tersebut. Hak cipta untuk program computer berlaku selama 50 tahun (Pasal 30). Harga program komputer/ *software* yang sangat mahal bagi warga negara Indonesia merupakan peluang yang cukup menjanjikan bagi para pelaku bisnis guna menggandakan serta menjual *software* bajakan dengan harga yang sangat murah. Misalnya, program anti virus seharga $ 50 dapat dibeli dengan harga Rp20.000,00. Penjualan dengan harga sangat murah dibandingkan dengan *software* asli tersebut menghasilkan keuntungan yang sangat besar bagi pelaku sebab modal yang dikeluarkan tidak lebih dari Rp 5.000,00 perkeping. Maraknya pembajakan *software* di Indonesia yang terkesan "dimaklumi" tentunya sangat merugikan pemilik hak cipta. Tindakan pembajakan program komputer tersebut juga merupakan tindak pidana sebagaimana diatur dalam Pasal 72 ayat (3) yaitu "Barang siapa dengan sengaja dan tanpa hak memperbanyak penggunaan untuk kepentingan komersial suatu program computer dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/ atau denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah) ".

c. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi

Menurut Pasal 1 angka (1) Undang-Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem

elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang-Undang ini, terutama bagi para *hacker* yang masuk ke sistem jaringan milik orang lain sebagaimana diatur pada Pasal 22, yaitu Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

a) Akses ke jaringan telekomunikasi

b) Akses ke jasa telekomunikasi

c) Akses ke jaringan telekomunikasi khusus

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi "Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)"

d. Undang-Undang No 8 Tahun 1997 tentang Dokumen Perusahaan

Dengan dikeluarkannya Undang-Undang No. 8 Tahun 1997 tanggal 24 Maret 1997 tentang Dokumen Perusahaan, pemerintah berusaha untuk mengatur pengakuan atas mikrofilm dan media lainnya (alat penyimpan informasi yang bukan kertas dan mempunyai tingkat pengamanan yang dapat menjamin keaslian dokumen yang dialihkan atau ditransformasikan. Misalnya *Compact Disk - Read Only Memory* (CD - ROM), dan *Write - Once - Read - Many* (WORM), yang diatur dalam Pasal 12 Undang-Undang tersebut sebagai alat bukti yang sah.

e. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-Undang ini merupakan Undang-Undang yang paling ampuh bagi seorang penyidik untuk mendapatkan informasi mengenai tersangka yang melakukan penipuan melalui Internet, karena tidak memerlukan prosedur birokrasi yang panjang dan memakan waktu yang lama, sebab penipuan merupakan salah satu jenis tindak pidana yang termasuk dalam pencucian

uang (Pasal 2 Ayat (1) Huruf q). Penyidik dapat meminta kepada bank yang menerima transfer untuk memberikan identitas dan data perbankan yang dimiliki oleh tersangka tanpa harus mengikuti peraturan sesuai dengan yang datur dalam Undang-Undang Perbankan. Dalam Undang-Undang Perbankan identitas dan data perbankan merupakan bagian dari kerahasiaan bank sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedur yang harus dilakukan adalah mengirimkan surat dari Kapolda ke Kapolri untuk diteruskan ke Gubernur Bank Indonesia. Prosedur tersebut memakan waktu yang cukup lama untuk mendapatkan data dan informasi yang diinginkan. Dalam Undang-Undang Pencucian Uang proses tersebut lebih cepat karena Kapolda cukup mengirimkan surat kepada Pemimpin Bank Indonesia di daerah tersebut dengan tembusan kepada Kapolri dan Gubernur Bank Indonesia, sehingga data dan informasi yang dibutuhkan lebih cepat didapat dan memudahkan proses penyelidikan terhadap pelaku, karena data yang diberikan oleh pihak bank, berbentuk: aplikasi pendaftaran, jumlah rekening masuk dan keluar serta kapan dan dimana dilakukan transaksi maka penyidik dapat menelusuri keberadaan pelaku berdasarkan data– data tersebut. Undang-Undang ini juga mengatur mengenai alat bukti elektronik atau *digital evidence* sesuai dengan Pasal 38 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optic atau yang serupa dengan itu.

f. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

Selain Undang-Undang No. 25 Tahun 2003, Undang-Undang ini mengatur mengenai alat bukti elektronik sesuai dengan Pasal 27 huruf b yaitu alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optic atau yang serupa dengan itu. *Digital evidence* atau alat bukti elektronik sangatlah berperan dalam penyelidikan kasus terorisme, karena saat ini komunikasi antara para pelaku di lapangan dengan pimpinan atau aktor intelektualnya dilakukan dengan memanfaatkan fasilitas di Internet untuk menerima perintah atau menyampaikan kondisi di lapangan karena para pelaku mengetahui pelacakan terhadap Internet lebih sulit dibandingkan pelacakan melalui handphone. Fasilitas yang sering digunakan adalah *e-mail* dan *chat room* selain mencari informasi dengan menggunakan *search engine* serta melakukan propaganda melalui *bulletin board* atau *mailing list*.

PENUTUP

Cybercrime atau kejahatan telematika adalah tergolong kejahatan transnasional (*trans-national crime*) karena dalam mejalankan aksinya aktor cybercrime (hacker) memanfaatkan teknologi internet sebagai media utama. Saat ini cybercrime telah menjadi masalah tidak hanya bagi satu negara tapi hampir seluruh negara, karena sifatnya yang transnasional. *Cybercrime* juga dapat digolongkan kedalam berbagai macam seperti kasus pornografi, teroris, pembobolan ATM dan lain sebagainya. Dalam peanggulangan secara global banyak poin-poin kesepakatan dari hasil konvensi-konvensi tersebut yang menghasilkan peraturan-peraturan cybercrime yang harus dipatuhi oleh masyarakat dunia. Di Indonesia, dengan berlakunya Undang-Undang Nomor 11 tahun 2008 mengenai Informasi dan Transaksi Elektronik, maka kita berharap agar Indonesia tidak lagi menjadi *"safe heaven"* bagi pelaku kejahatan telematika. Hal ini juga harus didukung oleh peningkatan pengetahuan atas teknologi informasi dan komunikasi baik dari para aparat penegak hukum misalnya polisi, hakim dan jaksa, juga adanya sosialisasi terhadap masyarakat berkaitan dengan kejahatan telematika itu sendiri.

DAFTAR PUSTAKA

David Berlind, "Reno's Border Patrol Made Ineffective," PC Week, April 8, 1996, hlm. 78.

Garda T. Paripurna, Sekilas Tentang Kejahatan Transnasional, Riset Hukum Kejahatan Transnasional, 2008,

Gerhard O. W. Mueller, "Transnational Crime: Definitions and Concepts," Transnational Organized Crime 4, no. 1998 (n.d.).

Havana, Cuba 27 August to 7 September 1990, A/Conf.144/7, 26 July 1990.

John R. Wagley, Transnational Organized Crime:Principal Threats and U.S. Responses" (Congressional Research Service, The Library of Congress, 2006).

Mark Findlay, The globalization of Crime: Understanding Transnational Relationship in Context (Cambridge University Press, 2003).

Martin, J. M. and Romano, A. T., Multinational Crime-Terrorism, Espionage, Drug & Arms Trafficking (SAGE Publications, 1992

Melissa Virus Exposes Computer Users' Vulnerability," *Japan Computer Industry Scan*, April 12, 1999,available at 1999 WL 9642279;

Muladi, Demokratisasi, Hak Asasi Manusia, dan Reformasi Hukum di Indonesia, 1st ed. (Jakarta: The Habibie Center, 2002).

Richard Power, ed., 2000, "2000 CSI/FBIComputerCrimeand Security Survey," *Computer Security Issues and Trends* 6, hlm. 3

See "Hackers Alter Romanian Money Rate," New York Times on the Web/ Breaking News from

United Nations, Changes in Forms and Dimensions of Criminality - Transnational and National, Working paper prepared by the Secretariat for the Fifth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Toronto, Canada, 1-12 September 1975).

Suspected Russia Hackers Held," New York Times on the Web/Breaking News from Associated Press,

United Nations, Eigth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,

DAFTAR LAMAN:

April 28, 2000, reported at _http://www.nytimes.com/ aponline/i/AP-Russia-Hackers.html_.

Associated Press, November 3, 1999, reported at _http:// www.nytimes.com/aponline/i/AP-Romania-Hackers.html_.

irmarr.staff.gunadarma.ac.id/.../files/.../Modus+Kejahatan+dalam+TI.doc

laluilmi.blogspot.com/.../modus-modus-kejahatan-dalam-it.html

vub.academia.edu/.../KEJHATAN_TELEMATIKA_SEBAGAI_KEJAHATAN_TRANSNASIONAL.pdf

www.scribd.com/doc/.../Definisi-Transnational-Crime

www.usdoj.gov/criminal/cybercrimes