TINDAK PIDANA TEKNOLOGI INFORMASI DAN PERKEMBANGANNYA

Oleh : AKBP. Drs. E. Brata Mandala*

A. PENDAHULUAN

Terminologi Cybercrime yang populer digunakan masyarakat dapat diartikan sebagai kejahatan di dunia maya atau tidak riil ini artinya sama saja dengan tidak ada tindak pidana atau kejahatan, karena suatu tindak pidana harus pasti objek dan subjeknya, Locus delicti serta tempus delictinya. Orang yang mengetik keyboard komputer adalah nyata begitu juga dengan komputer yang digunakan, terpus delicti bila dikonversikan ke sistim GMT_akan mendapatkan waktu yang pasti dan tepat begitu juga dengan locus delicti bisa di warnet atau sebuah rumah, jadi Locus delicti baik didalam, ataupun diluar negeri tidak nenjadi masalah.

Karena itu lebih tepat bila digunakan istilah tindak pidana di bidang informasi teknologi atau disingkat dengan Tindak pidana teknologi informasi[1], apabila dilihat dari modus operandinya akan nampak jelas terdiri dari dua bagian besar yaitu:

a. Kejahatan umum/biasa yang difasilitasi oleh teknologi informasi (sebelum ada teknologi informasi sudah ada dan biasa terjadi), atau dalam aksinya para kriminal menggunakan komputer/ media Internet sebagai sarana serta alat untuk melakukan kejahatan, contohnya Penipuan Kartu Kredit, Penipuan Internet Banking, pengancaman / Terrorisme, Pornografi, dsb.

b. Kejahatan yang sasaran/targetnya adalah fasilitas serta sistim teknologi informasi, para kriminal menggunakan sarana teknologi informasi untuk menyerang atau merusak sarana teknologi informasi lainnya yang menjadi target, pada posisi ini komputer / internet sebagai alat juga sebagai sasaran / korban.

* Penyidik pada Unit V Infotek-Direktorat II/ Ekonomi & Khusus Badan Reserse Kriminal Polri.

Secara umum lebih dikenal sebagai Hacking / Cracking yang menyerang program-program operasi jaringan computer, contohnya; trespassing, DDOS Attack, Defacing, Cracking and Phreaking serta penyerangan dengan Virus / Worms atau Program-program jahat lainnya.

B. SITUASI TINDAK PIDANA TEKNOLOGI INFORMASI 2002

Kejahatan ini berkembang di Indonesia cukup pesat seiring dengan penggunaan teknologi informasi, data terakhir yang dapat dicatat Polri adalah sebagai berikut :

Tabel 1

Kejahatan Umum Difasilitasi Tehnologi Informasi

No	MO	Total	Lokasi Korban	Lokasi Tersangka
01	Credit card Fraud	152	84 USA 25 canada 11 spain 8 Germany 8 Australia 4 British 3 Denmark 1 France 1 Austria 3 Japan 3 Singapura 1 Korea	62 Yogyakarta 43 Central Java 36 West Java 24 Jakarta 18 Sumatra 12 East Java 3 Kalimantan 3 Sulawesi 17 Lain-lain
02	Banking	4	1 Solo, 1 Yogya-karta, 2 Jakarta	2 USA, 1 Malaysia, 1 Australia
03	E-mail Threasts	2	1 Germany, 1 Australia	1 Bandung, 1 Yogyakarta
04	Terrorism	1	Australia, UK, USA, Japan, Korea dan lain-lain.	1 (Imam Samudra)
**	Grand Total	152	159	225

Tabel 2

Kejahatan dengan Sasaran Sistem & Fasilitas Tehnologi Informasi

No	MO	Total	Lokasi Korban	Lokasi Tersangka
01	DDOS Attacks	3	1 Japan 1 Denmark 1 Singapore	1 Jakarta 2 Bandung
02	Cracking	3	1 Singapore 2 Jakarta	2 Jakarta 1 Medan
03	Phreaking	1	1 Jakarta	1 Internet café Jakarta
04	Worms/Virus Attacks	1	Jakarta, Bandung	China?
**	**Grand Total**	7	7	7

Dari data tersebut kejahatan carding merupakan yang terbesar dan menyebabkan kerugian lebih dari US$ 1,296,597 atau Rp. 11.669.373.000,-(lebih dari 11,6 milyar rupiah !).

Kasus Yang Menonjol

Dari komputer atau laptop milik Imam Samudra (pelaku peledakan bom di Bali) yang dapat disita oleh penyidik Polri, dapat diketahui adanya hubungan yang antara aktifitas terorisme dan tindak pidana teknologi informasi serta penggunaan fasilitas internet untuk menunjang operasi kelompoknya. Electronic evidence yang dapat diungkap penyidik membuktikan bahwa internet digunakan oleh kelompok teroris untuk komunikasi, propaganda, pengancaman serta kegiatan carding dalam rangka mendapatkan dana atau memenuhi kebutuhan alat-alat elektronik yang mereka perlukan.

Karena itulah Imam Samudra sipelaku utama dalam kasus peledakan Bom di Bali pada tanggal 12 Oktober 2002 mendapat julukan "THE COMPLETE TERRORIST" karena memiliki kemampuan yang cukup dalam kegiatan perencanaan pemboman, dan mendisain elektronik device untuk Bomb trigger, perampok, carder, hacker dan website creator. Imam samudra membuat sendiri website "www.istimata.com" dan menggunakan cara carding untuk membayar hosting website tersebut, selain itu mengaku pernah melakukan hacking terhadap salah satu website di Israel karena membencinya.

C. PREDIKSI PERKEMBANGAN TPTI

1. Cyber Terrorism

Figur kejahatan ini pada tahun 2002 memang masih diwarnai oleh kejahatan carding serta ada yang menonjol sekali yaitu carding digunakan oleh para teroris dan internet digunakan untuk komunikasi para teroris khususnya kelompok Imam samudra, namun kasus ini belum dapat dikatakan cyber Terrorism sebagaimana yang didefinisikan oleh National Police Agency of Japan (NPA)[2] yaitu "electronic attacks throuh computer networks against critical infrastructures that have potential critical affects on social and economic activities of the nation".

Suatu negara dapat saja dijamin bebas dari kejahatan cyber terrorism dengan satu syarat "tidak ada sama sekali jaringan internet di negaranya", artinya bila internet atau teknologi infornasi telah digunakan disuatu negara maka potensi terjadinya cyber terrorism akan sangat besar terjadi pada negara tersebut. Karena itu Indonesia juga terancam dan sangat potensial akan terjadi sebab Internet dan Teknologi Informasi sudah merupakan kehidupan sehari-hari.

Memang saat ini serangan secara elektronik dengan menggunakan internet terhadap sasaran suatu jaringan komputer yang menunjang operasional suatu infrastruktur kritis yang dapat mengganggu secara langsung ekonomi negara serta kehidupan bernegara di Indonesia masih belum terjadi, namun kita harus sedini mungkin mewaspadainya karena makin banyaknya internet atau teknologi informasi digunakan pada infrastruktur kritis di Indonesia.

Cyber terrorism di Indonesia hanyalah masalah waktu saja atau "Time Being".

Pada suatu saat akan terjadi sebagaimana dialami oleh Amerika telah beberapa kali diserang[3], diantaranya pada bulan April dan Mei 2001 di California terjadi gangguan terhadap aliran listrik (PLN) sehingga diwilayah itu kehilangan pasokan tenaga listrik secara total akibat serangan hacker dari China[4].

2. Karakteristik Cyber Terrorism

Cyber terrorism bila tidak diamati secara teliti maka akan tampak sama dengan DdoS Attact, Hacking atau Cracking sebagaimana biasanya, namun ada beberapa perbedaan yang menonjol bila diteliti dari ciri-cirinya[5] sebagai berikut :

a. Modal utama menyerang relatif sangat murah, sebuah serangan

yang besar / luas namun cukup dengan hanya menggunakan komputer dan modem yang sederhana.

b. Dapat dilakukan oleh setiap individu, tidak perlu personil/ unit yang besar.

c. Rendahnya perkiraan terhadap resiko yang akan terjadi serta sangat sulit untuk melokalisir tersangka, bahkan kadang-kadang tidak menyadari sedang diserang.

d. Tidak ada batasan waktu dan tempat, sangat memungkinkan diserang kapan saja (setiap saat) dan dari manapun.

e. Kerugian akan sangat besar/ mahal dan meluas apabila serangan tersebut berhasil.

f. Motif untuk tujuan tertentu (bukan ubtuk tujuan keuntungan ekonomi saja).

g. Sasaran terfokus (disengaja) pada infrastruktur kritis.

Dapat disimpulkan perbedaannya adalah pada; motifnya, sasarannya serta dampak kerugian yang akan sangat besar serta fatal apabila serangannya berhasil.

3. Target Infrastruktur Kritis

Infrastruktur kritis adalah suatu institusi yang berperan sebagai sarana bagi masyarakat luas dalam menunjang kebutuhan hidupnya atau berfungsi melayani masyarakat luas agar kehidupannya dapat berjalan secara normal, artinya apabila institusi ini tidak berfungsi atau terganggu maka akan berakibat langsung pada kehidupan masyarakat secara luas dan mereka tidak dapat melangsungkan kehidupannya secara normal. Adapun contoh dari infratruktur kritis ini antara lain sebagai berikut :

a. Jaringan listrik, pasokan Gas, Air & BBM.

b. Jaringan kominfo, keuangan, pelayanan kesehatan.

c. Fasilitas penerbangan, kereta Api.

d. Pelayanan Kepolisian, kekuatan pertahanan dan pemerintahan.

CIAO (Critical Infrastructure Assurance Office)[6] di Amerika mendefinisikan infra struktur kritis adalah sebagai "Those systems and assets–both physical and syber–so vital to the Nation that their capacity or destruction would have a debilitating impact on national security, national economic security and / or national public health and safety", mengacu pada definisi ini dapat disimpulkan bahwa apabila salah satu atau sebagian dari infra struktur kritis tersebut menjadi target atau sasaran

cyber terrorism maka dampaknya akan sangat luas bagi masyarakat dan kerugiannya akan sangat besar, jadi pada tempatnya bila dalam draft cyberlaw diberikan perlakuan khusus dalam hal perlindungan terhadap infrastruktur kritis serta hukuman yang lebih keras terhadap pelakunya.

D. STRATEGI PENANGGULANGANNYA

Berpijak pada dari ciri-ciri serangga cyber yang tidak cepat terpantau atau disadari oleh korbannya (unsur pendadakan yang tinggi) kapan saja dapat terjadi dan dapat diserang dari tempat manapun di dunia ini, dengan modal yang relatif murah. Maka diperlukan suatu strategi yang dapat memberikan peringatan secara dini akan terjadinya serangan, serta kecepatan bereaksi untuk menagkal atau menanggulangi serangan tersebut.

National Police Agency of Japan (NPA) telah membentuk Cyber Taskforce untuk menjawab tantangan ini, dikombinasikan dengan membangun suatu instalasi berupa sistem pemantau gangguan sacara cepat yang dapat memberikan peringatan dini serta informasi lokasi korban penyerangan juga lokasi darimana pengganggu berasal, sistem ini disebut Real time Intrusion Detection System Network (Real time IDS Network). Di Amerika pada bulan Februari 2003 dilunsurkan The Nation Strategy for The Physical Protection of Critical Infrastructures and Key Assets serta The National Strategy to Secure Cyberspace, kita sekarang sudah perlu untuk mengadopsi sistem ini dan Mabes Polri akan mengembangkan serta membangunnya.

1. Cyber Taskforce Center / CTF

Cyber taskforce adalah suatu gugus tugas yang dirancang untuk menghadapi aspek-aspek tehnis serta respon darurat bila terjadi serangan cyber (tindak pidana biasa di internet terutama cyber terrorism), dengan peran mulai dari pencegahan kerusakan yang lebih meluas, assitensi dan recovery korban serta penyidikan untuk mengungkap pelakunya. Cyber Taskforce Center berada di Mabes Polri serta ada pada setiap Polda, didukung dan terkordinasi dengan komponen / institusi dibidang teknologi informasi diluar Polri antara lain; Kampus, Departemen terkait (Birokrat), Icon-icon teknologi informasi (Id-Cert, Id-First, dsb) serta industri di bidang Teknologi Informasi (APJII, AWARI, dsb).

a. Misi dan Peranannya

Misi Cyber Taskforce adalah "mencegah serta merespon keadaan

darurat agar kerugian / resiko akibat serangan pada sistem informasi terhadap infra struktur kritis seminimal mungkin serta melakukan tindakan hukum yang diperlukan", dengan peran sebagai berikut :

(a) Pusat komando & informasi;
(b) Membangun hubungan kerja yang baik dengan infrastruktur kritis;
(c) Mengumpulkan / menganalisa informasi;
(d) Merespon segera situasi darurat untuk memperkecil kerusakan;
(e) Intrusion Detection System.

b. Kegiatan Cyber Taskforce Center

Cyber Taskforce melakukan kegiatan-kegiatan yang spesifik dalam upaya untuk merealisasikan peran-nya, antara lain sebagai berikut :

(a) Mendeteksi secara dini dan memberikan bantuan untuk meminimalkan kerawanan-kerawanan pada infrastruktur kritis,
(b) Merespon secara cepat keadaan darurat agar kerusakannya minim,
(c) Menyediakan bimbingan & bantuan investigasi serta melakukan investigasi secara langsung.

c. Mengapa diperlukan

Cyber Taskforce Center mutlak diperlukan dan harus segera diwujudkan, tentunya dengan dukungan dan keterlibatan dari berbagai pihak karena bagaimanapun juga Polri tidak dapat berdiri sendiri menghadapi fenomena Hightech crime yang sarat atau penuh dengan disiplin ilmu diluar Ilmu Kepolisian, juga sarat dengan sarana (hardware & software) yang pengadaannya ada pada industri-industri diluar institusi Kepolisian. Adapun beberapa pertimbangan atau alasan kuat perlunya Cyber Taskforce dibentuk adalah sebagai berikut;

(a) Indonesia akan menuju e-Government, artinya insfrastruktur kritis akan semakin bertambah.
(b) Kejadian-kejadian Web page defacement dari e-Government di Indonesia sudah sering terjadi oleh Hacker terorganisasi dari luar negeri (Perang Cyber).
(c) Bukti-bukti pada kasus Imam Samudra yang membuktikan bahwa Cyber terrorism sekarang ini sudah pada tahap "clear and present danger" walaupun masih belum berupa electronic attack.
(d) IP Address Indonesia diblokir di beberapa negara, akibat dari kelemahan dalam pencegahan tindak pidana di bidang technologi informasi dan kelemahan penegakan hukumnya.

(e) Sangat diperlukan untuk upaya preventif dan memperkecil kerusakan serta mengorganisasikan staff yang telah terlatih dibidang tehnis.

(f) Sebagai saluran keluhan dan pengaduan yang selama ini selalu dicari-cari oleh masyarakat, terutama para korban TPTI.

Cyber Taskforce Center ini hanya dapat berfungsi dengan baik apabila telah dibangun (installed) Real Time IDS Network), atau harus dibangun keduanya secara bersamaan.

2. Real Time Instruction Detection System Networak (Real Time IDS Network)

Konsep ini berasal dari NPA-Japan yang dijelaskan Mr.Satsuki Suwa, Assistant Director Cyber Terrorism Technology office pada pertemuan tahunan CTINS (Computer crime & Technology Information Network System) di Tokyo 26-29 Maret 2002, Real Time IDS Network merupakan instalasi dari berbagai komponen yang terintegrasi guna menciptakan sistim peringatan dini dari gangguan/ serangan elektronik serta agar tercipta suatu rekasi yang cepat untuk menanggulangi gangguan atau serangan tersebut. Komponen-komponen system ini membentuk suatu jaringan kerja (network) yang melakukan tugas sesuai peran dan fungsinya masing-masing namun terintegrasi sehingga laporan dapat cepat disampaikan, demikian juga dalam menanggulangi gangguan atau serangan yang terjadi komponen ini-pun berfungsi dan berperan secara proposional / tidak terjadi duplikasi tetapi saling mengisi dan terkordinir dengan baik.

a. Komponen dan Peran

Komponen system ini terdiri dari komponen pengguna atau user, backtone atau komponen tulang punggung, komponen tehnis dan pusat informasi sekaligus early warning, komponen OSI (Open Source Intelligent), serta komponen Infra struktur kritis. Adapun peran dari masing-masing komponen tersebut adalah sebagai berikut;

(a) Komponen pengguna adalah Cyber Taskforce Center di Mabes Polri dan Kewilayahan (Polda sampai ke Polres) akan tetapi unsur / komponen lainnya juga bisa jadi pengguna karena diberikan akses langsung tetapi dengan kasitas terbatas. Adapun peranannya ada dua yaitu;

- Mengkordinasikan dan mengintegrasikan komponen IDS Network;
- Menerima dan menganilisa informasi serta memanfaatkannya untuk tindakan cepat berupa bantuan, penanggu-

langan ataupun tindakan hukum (penyidikan).

(b) Komponen Backbone atau tulang punggung yang menjadi pijakan dari opersionalnya Cyber Taskforce, komponen ini antara lain adalah;
- Menkoinfo yang berperan dalam mengeluarkan kebijakan-kebijakan yang menjadi landasan operasional.
- Menhub cq Direktorat Jenderal Pos & Telekomunikasi (Dirjen Postel) yang berperan dalam segi tehnis dan perijinan dibidang technologi informasi

(c) Komponen Tehnis antara lain ID-CERT, ID-FIRST, AP JII serta institusi lainnya, dengan peran antara lain;
- Sebagai gerbang informasi mulai dari pengumpulan, pengolahan dan analisa data yang akan disajikan pada User yang memerlukan;
- Pusat deteksi dan early warning sekaligus menyajikan saran atau rekomendasi tindakan;
- Bantuan tehnis dalam upaya pencegahan serangan, bantuan peulihan kerusakan dan asistensi penyidikan (electronic evidence collection & source serta IT expert withness/forensic)

(d) Komponen OSI (Open Source Intelligent) antara lain; masyarakat Telekomunikasi atau Teknologi Informasi, AWARI serta komponen lainnya yang terkait dengan penggunaan teknologi informasi, dengan peran memberikan informasi atau masukan baik secara langsung atau pun tidak langsung.

(e) Komponen Infra Struktur Kritis yang akan berperan sentral dalam early warning dan deteksi karena posisinya potensial sebagai target dari suatu serangan yang akan datang secara tiba-tiba, dengan peran memberikan informasi secara priodik dan informasi yan greal time terjadinya suatu serangan / gangguan termasuk memberikan electronic evidence yang diperlukan kepada penyidik (CTF). Apabila menjadi korban.

b. Konsep Instalasi dan Hubungan Tata Cara Kerja / HTCK

Seluruh komponen-komponen tersebut harus terhubung secara permanen dalam satu saluran khusus atau menggunakan broadband khusus agar bisa terwujud sistim laporan, information exchange dan monitoring, 24H / 7D, sebelumnya harus menentukan sistem apa yang akan dipakai bersama agar bisa saling berhubungan denga lancar atau tidak terhabat. Pada masing-masing komponen.

Komponen user atau CTF di Mabes Polri melakukan monitor bersama dengan komponen tehnis, sementara itu komponen OSI secara periodik memberikan masukan serta informasi yang akan disampaikan pada komponen infrastruktur kritis melalui komponen tehnis atau CTF tergantung dari topik atau masalahnya. Pada sistem ini harus diinstall juga sistem peringatan atau "Alert system" agar bila terjadi sesuatu gangguan atau serangan dapat segera disebarkan pada semua komponen, bila hal ini terjadi secara otomatis masing-masing komponen akan bereaksi / beraksi sesuai dengan perannya masing-masing.

c. Hubungan dengan infrastruktur kritis

Komunikasi yang terus menerus adalah dasar atau prinsip dari Real time IDS Network artinya tidak boleh terputus harus tersambung dan termonitor secara 24 H / 7D, selain menggunakan sarana teknologi informasi juga harus ada Point of contact serta Person of contact yang telah ditetapkan sebelumnya pada setiap komponen, terutama pada komponen infrastruktur kritis. Adapun pemanfaatan dan kegiatannya antara lain adalah;

(a) Tukar menukar informasi / information exchange untuk pengumpulan & analisis informasi guna menagkal Cyber Terrorism.
(b) Bimbingan dan pelayanan sistem keamanan informasi,
(c) Bimbingan untuk crime prevention,
(d) Permintaan / pengumpulan electronic evidence secara cepat / tepat (legal dapat diterima dipengadilan),
(e) Respon darurat untuk memperkecil kerusakan.

Seluruh konsep tersebut diatas memerlukan kerjasama interdepartmental dan melibatkan komponen-komponen dalam masyarakat teknologi informasi diluar birokrat terutama industri dibidang teknologi informasi,serta hanya dapat terwujud bila ada komitmen untuk mewujudkannya juga bila tersedia dana yang cukup besar. Artinya rencana ini tidak dapat hanya dilakukan oleh satu instansi pemerintah saja (Polri) tetapi harus diangkat ke lembaga yang lebih tinggi yaitu presiden, karena pengembangan dan keamanan teknologi informasi merupakan kewajiban bagi setiap negara yang meratifikasi United Nation General Assembly (UNGA) No. 55/63 tanggal 4 Desember 2001[7] termasuk Indonesia.

E. KESIMPULAN DAN SARAN

1. Kesimpulan

Tindak pidana dibidang teknologi

informasi yang terjadi di Indonesia sudah pada tahap yang memerlukan penanganan yang serius dan dampaknya cukup buruk antara lain IP Address yang berasal dari Indonesia diblokir dibeberapa negara, juga terbukti salah satu kelompok teroris di Indonesia telah menggunakan sarana teknologi informasi dalam menunjang kegiatan operasinya.

Infrastruktur kritis di Indonesia akan semakin banyak memanfaatkan teknologi informasi dan hal ini merupakan Police Hazard atau petensi terjadinya serangan Cyber Terrorism di Indonesia, karena serangan ini unik / spesifik terjadi di Cyberspace maka menangkalnya harus dengan cara-cara yang khusus pula diantaranya dengan mewujudkan Cyber Taskforce Center (CTF) dikombinasikan dengan Real time IDS Network.

Disadari bahwa mewujudkan kedua hal tersebut di atas tidaklah mudah karena perlu melibatkan interdepartmental serta komponen-komponen lainnya yang terkait dan perlunya "komitmen" bersama, karena itu masalah ini perlu diteruskan ke lembaga yang lebih tinggi dari Departemen yaitu Presiden sebab sudah bersifat "National Wide" bahkan "International Wide" yang tidak akan mungkin dipecahkan hanya oleh salah satu departemen saja.

2. Saran-saran

Studi banding perlu dilakukan secara bersama-sama baik dengan cara literature studi ataupun working visit, terutama ke Jepang yang telah establish dalam mengoperasionalkan Cyber Taskforce Center (CTF) dan Real time IDS Network serta cukup maju dalam bidang teknologi informasi di Asia. Team study ini harus terdiri dari berbagai unsur departemen dan komponen-komponen lainnya yang terkait dengan teknologi informasi di Indonesia.

Menyiapkan dan mewujudkan M.O.U (mutual of understanding) antara departemen yang terkait serta menentukan project officer yang dikedepankan agar tidak terjadi duplikasi, dengan cara merancang hubungan cara kerja (HTCK) yang jelas serta mengikat bagi yang terlibat di dalamnya.

—oOo—

Catatan :

halaman berikutnya

Catatan :

[1]International Law Enforcement Academy (ILEA) , FBI Computer Crime Investigation Handbook. Unpublished. Bangkok, 2001, hal. 100.

[2] Suwa Satsuki . Response the National Police Agency in Japan in Dealing with Cber Teroorism. Higtech Crime Devision NPA Japan. Unpublished. Tokyo, 2000.

[3]The White House. Defending America's Cyberspace- National Plan For Information System Protection V.1-An Invitation to a Dialogue. Washington DC-2000

[4]Suwa Satsuki. Ibid. Hal. 4.

[5]Suwa Satsuki. Ibid. Hal. 2.

[6]Critical Infrastructure Assurance Office. The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. Washington, DC – February 2003.

DAFTAR PUSTAKA

APEC., *Apec Tel 26 th Agenda*. Moskow – Russia, 15 – 18 August 2002

CNN dotcom. *Bracing for Guerrilla Warfare in Cyberspace* , [online]. Available : http://cnn.com/TECH/specials/hackers/cyberterror/. 15 February 2000.

Critical Infrastructure Assurance Office. *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC – February 2003.

International Law Enforcement Academy (ILEA). *FBI computer Crime Investigation Handbook*. Unpublished, Bangkok – 2001.

NW3C. *About The National White Collar Crime*. [on line]. Available: http://www.nw3c.org. 10 October 2002.

Sabadan Daan dan Kunarto. Kejahatan Berdimensi Baru. Jakarta: Cipta Manunggal, 1999.

Suwa Satsuki. *Response of the National Police Agency in Japan in Dealing with Cyber Terrorism*. High Tech Crime Division NPA Japan. Unpublished. Tokyo, 2002.

The White House. *Defending America's Cyberspace National Plan For Information Systems Protection V.1 An Invitation to a Dialogue*. Woshington DC- 2000.