027

# DAMPAK TEKNOLOGI KOMUNIKASI DAN INFORMASI TERHADAP KEGIATAN TERORISME*

**Oleh: Cahyana Ahmadjayadi**

## PENDAHULUAN

Salah satu sarana untuk mewujudkan masyarakat sejahtera sebagaimana diamanatkan dalam Pancasila dan Undang-Undang Dasar 1945, adalah pemanfaatan teknologi khususnya komunikasi dan informasi yang lazim dikenal dengan istilah ICT *(Information and Communication Technology)* secara aman, optimal, merata dan menyebar ke seluruh lapisan warga negara Indonesia.

Bahwa, perkembangan Teknologi Informasi (TI) dalam dasawarsa terakhir mempengaruhi segala aspek kehidupan manusia, mulai dari ekonomi, budaya, dan politik. Di beberapa negara ada yang menggunakan moment perkembangan TI ini sebagai basis dan revolusi industri dan kebangkitan ekonomi, yang pada saatnya nanti akan membawa perubahan drastis derajat kehidupan ekonomi rakyatnya.

Pemanfaatan teknologi komunikasi dan informasi di samping memberi manfaat bagi kemaslahatan masyarakat, di sisi lain memiliki peluang untuk digunakan sebagai alat untuk melakukan kejahatan.

Kejahatan yang dilakukan menggunakan teknologi komunikasi dan informasi dapat terjadi pada kejahatan kriminal biasa maupun yang secara khusus menargetkan kepada sesama infrastruktur teknologi komunikasi dan informasi sebagai korbannya, di mana dampak dari kejahatan yang muncul dari penggunaan teknologi komunikasi dan informasi secara negatif dapat menyebabkan ambruknya tatanan sosial, lumpuhnya perekonomian nasional, lemahnya sistem pertahanan dan keamanan, serta memliki peluang untuk digunakan sebagai alat teror.

Hingga saat ini perangkat peraturan dan perundangan yang tersedia belum dapat mengakomodasi penindakan terhadap kejahatan di bidang teknologi komunikasi dan informasi. Cyber Laws kita masih dalam taraf pemrosesan berupa Rancangan Undang-Undang dan masih memerlukan penyempurnaan-

*) Makalah disampaikan pada Seminar Tentang Penegakan Hukum Terhadap Terorisme, diselenggarakan oleh BPHN Departemen Kehakiman dan HAM bekerjasama dengan Fakultas Hukum Universitas Padjadjaran Bandung, tangal 13-14 Oktober 2003.

penyempurnaan dan harus berpacu dengan perkembangan teknologi komunikasi dan informasi yang sangat cepat.

Patut diakui, bahwa hukum belum mampu mengimbangi pesatnya perkembangan teknologi komunikasi dan informasi, sehingga terkesan hukum selalu tertinggal oleh konvergensi teknologi komunikasi dan informasi. Hal ini bukan berarti kejahatan cyber atau kejahatan di dunia maya tidak dapat diatasi.

Sudah terbukti bahwa kejahatan dunia maya tidak saja berupa kejahatan konvensional *(old crime)* yang difasilitasi oleh new technology, akan tetapi sudah berkembang menjadi new crime - new technology. Demikian pula, kegiatan untuk menebar teror, tidak saja dilakukan melalui dunia nyata, akan tetapi sudah berpindah ke dunia maya *(cyber space)*, bahkan dampaknya jauh lebih dahsyat dibanding teror yang dilakukan di dunia nyata.

Tidak pernah terbayangkan sebelumnya, jika seandainya para teroris menguasai salah satu infrastruktur vital yang berdampak pada hajat hidup orang banyak, misalnya; teroris mampu mengacaukan sistem, pertahanan keamanan nasional dan mengendalikan seluruh persenjataan mutakhir dan menggunakan sesuai keinginan kelompoknya, atau para teroris mampu mengacaukan sistem perbankan nasional, bahkan sistem penerbangan, listrik, kepolisian, kominfo, pertambangan dan infrastruktur strategis lainnya.

Sepintas memang seperti mustahil, jika dilihat ke masa depan, perkembangan teknologi komunikasi dan informasi akan semakin kental dalam sendi-sendi kehidupan bermasyarakat, berbangsa dan bernegara. Sebab di masa datang akan semakin banyak dibangun infrastruktur strategis, seperti pembangunan e-government atau pemerintahan elektronik yang akan dibangun oleh pemda dan pemerintah pusat, dan hubungan kehidupan manusia modern tidak akan bisa dilepaskan dari dunia ICT.

Kegiatan terorisme di cyber space tidak saja berupa teror langsung, akan tetapi digunakan juga sebagai alat komunikasi melalui e-mail, propaganda, hacking, carding, mengacaukan informasi (memutar balikkan fakta), dsb.

Dunia teror sifatnya global, artinya teroris bukanlah berupa perorangan, akan tetapi sudah merupakan kelompok atau organisasi yang sistematis dan bersifat internasional. Serta didukung oleh pendanaan yang luar biasa besarnya dan jaringan multi nasional yang sangat rapi.

Teroris tertarik pada dunia cyber, karena sifat cyber space yang dapat menembus ruang dan waktu, tidak ada batas negara, tidak mengenal yurisdiksi, dan teror dapat dilakukan dari mana saja dan kapan saja.

## KONDISI SAAT INI

Internet ataupun teknologi komunikasi dan informasi/ICT memiliki sisi gelap dan sisi terang. Dari sisi terang, teknologi informasi membawa manfaat besar bagi umat manusia. Namun dari sisi gelap, teknologi informasi akan membawa bencana bagi umat manusia itu sendiri, jika tidak ada upaya untuk mempersempit ruang sisi' gelap tersebut. Bisa dari sisi gelap tersebut adalah:

A. INTERNET MEMBAWA DAMPAK NEGATIF DALAM BENTUK MUNCULNYA JENIS KEJAHATAN BARU
   - Hackers membobol komputer milik bank dan memindahkan dana secara melawan hukum
   - Kriminal mendistribusikan gambar pornografi anak
   - Teroris menggunakan Internet untuk merancang dan melaksanakan serangan
   - Penipu menggunakan kartu kredit milik orang lain untuk berbelanja melalui Internet

B. MUNCUL KEKHAWATIRAN AKAN ADANYA SERANGAN TERHADAP INFRASTRUKTUR STRATEGIS YANG VITAL.
   - Hackers mengacak sistem perbankan, pengendalian lalu lintas udara, distribusi listrik, jaringan telekomunikasi, jaringan keamanan dan pertahanan, jaringan polisi, kominfo, pertambangan, kesehatan, dll, yang berpotensi mengarah kepada bentuk terorisme.

C. PERTUMBUHAN EKONOMI DI ERA GLOBALISASI INFORMASI AKAN DIWARNAI OLEH MANFAAT DARI ADANYA:
   - e-commerce
   - e-government
   - Foreign Direct Investment (FDI)
   - Industri Penyediaan informasi
   - Pengembangan UKM

D. SEMUA MANFAAT DI ATAS DALAM KONDISI BAHAYA JIKA TIDAK DIDUKUNG OLEH PERANGKAT HUKUM DI BIDANG TI DAN GUGUS TUGAS (TASKFORCE) YANG SECARA KHUSUS MENANGANI TINDAK PIDANA BERBASIS TEKNOLOGI INFORMASI, GUNA PENGAMANAN INFORMASI ITU SENDIRI, KARENA :

- Ketergantungan Komputer dan jumlah komputer yang digunakan semakin bertambah
- Setiap Sistem mempunyai kelemahan (Vulnerabilities) yang bisa di-exploit
- Nilai Informasi Semakin Berharga/Tinggi
- Jumlah Operator Komputer Semakin Bertambah
- Jaringan.Sistem Semakin Luas
- Tehnik Hacking/Cracking Semakin Dipermudah (otomatis) Dengan Software
- Hukum Kurang Menjangkau Kejahatan Teknologi Informasi (Cyber Crime; RUU-ITE -"Cyberlaw"- masih dalam proses)
- Kecenderungan Mengabaikan Sikap Waspada Terhadap Penggunaan Konfigurasi Keamanan Jaringan
- Teknologi Sekuriti Selalu Tertinggal Dibanding Dengan Teknologi Informasi
- Kebijakan Sekuriti Intern untuk Organisasi tidak ada atau kurang diterapkan
- Belum ada manajemen yang melakukan aksi preventif yang pro-aktif
- Semakin banyaknya jaringan komputer yang terhubung ke Internet
- Indonesia segera akan menuju pada penerapan e-Government, dan akan semakin banyak infrastruktur strategis akan menjadi target kejahatan teknologi informasi.

Saat ini, khususnya di Indonesia, belum ada kasus yang menonjol tentang Cyber Terorism. Namun di masa datang, dengan maraknya pertumbuhan infrastruktur vital yang strategis, akan berpotensi melahirkan kejahatan terorisme yang difasilitasi oleh teknologi informasi.

Untuk kasus yang menonjol, dari Laptop Imam samudra yang disita oleh Polisi (pelaku peledakan Bom di Bali tanggal 12 Oktober 2002), diketahui adanya hubungan yang kuat antara aktivitas terorisme dan tindak pidana yang berbasis teknologi informasi, dengan fasilitas internet untuk menunjang operasi kelompoknya. Dari kasus Imam Samudra ini dapat dilihat bahwa Internet digunakan oleh kelompok teroris untuk komunikasi, propaganda, pengancaman, serta kegiatan carding dalam upaya mendapatkan dana atau pemenuhan alat-alat yang dapat digunakan untuk teror.

Kasus lainnya adalah di Amerika, pada bulan April dan Mei 2002 di California, telah terjadi gangguan aliran listrik, sehingga wilayah tersebut kehilangan pasokan tenaga listrik secara total, akibat serangan Hacker dari China.

Walaupun peristiwa teror di Bali pada tanggal 12 Oktober 2002 belum dapat dikatakan sebagai Cyber Terorisme, namun arah menuju ke cyber terorisme sudah menampakan diri. Seperti yang telah disebutkan di atas, bahwa Imam Samudra telah menggunakan teknologi informasi dan komunikasi sebagai sarana kegiatan terornya, namun belum 100% melakukan teror melalui dunia maya. Untuk itu pemerintah telah mengantisipasi peristiwa teror untuk masa datang dengan mengeluarkan Peraturan Pemerintah Pengganti Undang-Undang Republik Indonesia Nomor: 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme dan Peraturan Pemerintah Pengganti Undang-Undang Republik Indonesia No: 2 Tahun 2002 Tentang Pemberlakuan Peraturan Pemerintah Pengganti Undang-Undang Republik Indonesia No: 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Pada peristiwa peledakan Bom Di Bali Pada Tanggal 12 Oktober 2002.

Walaupun di dalam kedua Perpu tersebut di atas tidak disebut secara ekplisit tentang definisi "tindak pidana terorisme berbasis teknologi informasi", namun dalam pasal 27 Perpu No: 1 Tahun 2002 tersebut, telah mengarah pada penerimaan alat bukti elektronik (electronic evidence) sebagai alat bukti yang sah dan sejajar seperti yang dimaksud dalam Hukum Acara Pidana, bahwa "Alat Bukti" elektronik, seperti informasi yang dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu, dan data yang terekam secara elektonik.

Alat bukti elektronik ini bisa merupakan hasil teknologi komunikasi dan informasi dengan sarana internet *(Hi Tech Online)*, atau bisa juga merupakan hasil dan produk elektronik konvensional, seperti suara yang direkam melalui "tape recorder" biasa.Pasal ini masih merupakan pasal karet yang bisa diinterpretasikan dari berbagai sudut pandang, karena tidak secara khusus menyebut alat bukti elekronik dari hasil tindak pidana berbasis teknologi informasi.

Terciptanya Kedua Perpu di atas, merupakan komitmen pemerintah untuk mewujudkan ketentuan *Pasal 3 Convention Against terorrist Bombing (Tahun 1997) dan Convention On The Suppression of Financing Terorism (Tahun 1999)*, sebagai antisipasi tentang pendanaan untuk kegiatan teroris sebagai tindak pidana terorisme, sehingga sekaligus juga memperkuat Undang-Undang Nomor 15 tahun 2002 tentang Tindak Pidana Pencucian Uang. Di samping

itu, juga memuat ketentuan khusus tentang perlindungan hak asasi tersangka/ terdakwa yang disebut *"safe guarding rules"*, ketentuan ini merupakan lembaga hukum baru dalam Hukum Acara Pidana yang disebut *"hearing"* dan berfungsi sebagai lembaga yang melakukan *"legal audit"* terhadap seluruh dokumen atau laporan intelijen yang disampaikan oleh penyelidik yang menetapkan diteruskannya atau tidak suatu penyidikan atas dugaan adanya tindakan terorisme. Di lain sisi, Perpu tersebut juga memuat ketentuan yang memungkinkan Presiden membentuk satuan tugas anti teror yang dilandasi prinsip transparansi dan akuntabilitas publik *(sunshine principle)* dan prinsip pembatasan waktu efektif *(sunset principle)* guna menghindari penyalahgunaan wewenang yang dimiliki oleh satuan tugas tersebut.

Cyber terorisme sepintas akan tampak sama seperti cyber crime atau tindak pidana teknologi informasi biasa. Tapi jika diamati ada kekhususan yang dimiliki, yakni:

1. Motif, yakni bukan bertujuan untuk keuntungan pribadi atau ekonomi saja, namun lebih cenderung ke motif politik.
2. Sasaran atau targetnya, sangat berbeda dengan kejahatan teknologi informasi biasa, cyber terorist akan lebih memilih sasaran infrastruktur startegis dibanding menyerang website pribadi atau website atau infrastruktur yang tidak ada kaitannya dengan hajat hidup orang banyak.
3. Kerugian yang ditimbulkannya jika serangan berhasil, jauh lebih dahsyat dibanding sekadar cyber crime konvensional.
4. Serangan dilakukan secara terorganisir dan multi nasional, artinya jaringan teroris bisa terdiri dari negara-negara tertentu, yakni lebih dari satu negara.
5. Pola serangan dengan cakupan luas dan besar dengan dampak kerugian ke masyarakat luas.

**DEFINISI**

Belum ada definisi yang tepat dalam hukum nasional tentang Tindak Pidana Terorisme Berbasis Teknologi Informasi/ICT, yang merupakan dampak dari pemanfaatan teknologi komunikasi.dan informasi terhadap kegiatan terorisme, namun NPA telah merumuskannya sebagai : *"Serangan elektronik melalui network komputer terhadap infrastruktur kritis yang berpotensi besar mengganggu aktivitas sosial dan ekonomi bangsa/negara."*

Secara umum Cyber Terorism merupakan kejahatan yang berbasis komputer. Seperti misalnya yang didefinisikan oleh :

- The U.S. Department of Justice: "...any *illegal act* requiring *knowledge of computer technology for its perpetration, investigation, or prosecution'.*
- OECD: *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of date".*
- Andi Hamzah (1989): *"kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal"*

Definisi tentang kejahatan terorisme seperti yang disebutkan dalam Pasal 6 Perpu No: 1 tahun 2002, yakni : "Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal, dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau nengakibatkan *kerusakan atau kehancuran terhadap objek-objek vital yang strategis* atau lingkungan hidup atau fasilitas publik atau fasilitas internasional".

Untuk objek-objek vital yang strategis, dapat berupa infrastruktur-infrastruktur yang berbasis teknologi informasi, di mana kemungkinannya sangat tinggi dapat diserang oleh teroris melalui teknologi informasi pula. Sehingga kerusakannya lebih cenderung kepada perangkat lunak (software) dan aplikasinya, namun memiliki dampak politis, ekonomis, keamanan, pertahanan dan ketertiban, serta dampak sosial dan psikologi lainnya.

Unsur-unsur dari sebuah kegiatan terorisme, yakni:

- Adanya Kekerasan
- Adanya ancaman kekerasan
- Adanya suasana teror
- Adanya korban secara massal dalam wujud merampas kemerdekaan, hilangnya nyawa, rusak dan hancurnya infrastruktur-infrastruktur vital yang strategis. Lingkungan hidup dan fasilitas publik.

Pada umumnya, kegiatan terorisme adalah suatu kejahatan konvensional yang dilakukan di dunia nyata. Namun, karena perkembangan teknologi komunikasi dan informasi, modus operandi terorisme dapat beralih menggunakan pemanfaatan teknologi komunikasi dan informasi yang memiliki dampak teror ke masyarakat luas yang tidak kalah seperti terorisme di dunia nyata. Modus operandinya bisa 100% menggunakan teknologi informasi, namun dampak atau akibat terornya terjadi di dunia nyata. Delik semacam ini dapat

dikategorikan delik semi online, karena cara kerjanya ada di dunia maya (cyber) namun target dan dampaknya ada di dunia nyata.

Kejahatan yang berbasis teknologi informasi dapat dikategorikan dalam delik-delik di bawah ini :

DELIK SEMI ONLINE:

- *Carding :* Pencurian, Penipuan menggunakan komputer dan Internet *(fraud)*
- Akses kepada komputer dengan cara melawan hukum *(illegal acces)*
- Perusakan, dan atau Pencurian Data pada suatu komputer atau jaringan komputer tertutup *(forgely)*

DELIK ONLINE :

- Wiretapping
- Hacking
- Spamming
- Cybersquatters
- Virus Attack
- DoS
- Defacing
- Domain Hijacking
- Treespassing
- Illegal acces
- Illegal Interception
- Data Interference
- System Interference
- Cyberpornography
- Dll.

Kegiatan terorisme yang difasilitasi oleh teknologi komunikasi dan informasi sudah termasuk ke dalam "kejahatan" teknologi informasi, menjadi bentuk kejahatan baru di dunia maya, dengan sebutan "CyberTerorism". Cyber terorisme pada dasarnya merupakan kejahatan berbasis teknologi informasi biasa yang umum dikenal dengan "cyber crime". Namun karena motif, sasaran/ target, kerugian dan pola serangannya memiliki daya teror dan kerugian di

masyarakat luas yang luar biasa, maka delik ini menjadi delik yang patut dicermati oleh pemerintah dan masyarakat teknologi informasi, baik secara nasional, regional dan internasional.

Di masa depan, kegiatan terorisme yang difasilitasi teknologi komunikasi dan informasi akan menjadi sarana strategis bagi teroris guna melancarkan aksinya. Melakukan teror melalui fasilitas teknologi informasi memiliki keunggulan-keunggulan dan kemudahan tertentu bagi yang bersangkutan tanpa terbatas ruang, waktu, dan yurusdiksi, tanpa dirasakan dan diketahui secara dini oleh target (objek), dan saranya relatif murah hanya dengan modem biasa dan pengetahuan penyusupan yang memadai. Sasarannya jelas infrastruktur strategis yan vital, misalnya pangkalan angkatan udara, sistem pertahanan dan pengendalian Bom Nuklir dan persenjataan lainnya, pasokan listrik nasional, sistem pengendalian penerbangan sipil, sistem bank Sentral, Sistem transaksi elektronik, sistem pertambangan, sistem pasokan air dan pengendalian bendungan, sistem pasar modal, sistem database kesehatan, pendidikan, dan lain-lain yang berpotensi memiliki bias kekacauan secara politis, ekonomis dan keamanan nasional.

Tehnik hacking pada dasarnya adalah tehnik yang sangat sulit. Sang hacker dituntut harus memiliki keterampilan hacking dan cracking yang prima. Namun, berkat kemajuan teknologi perangkat lunak, tehnik hacking dan cracking dapat dipermudah dengan hacking tools yang jumlahnya sangat banyak dan berfariasi sesuai dengan tujuan serangannya dan tersebar luas di pasar bebas dan internet.

Tidak ada satupun sistem jaringan komputer/internet yang paling sempurna di dunia ini. Setiap sistem memiliki lubang-lubang keamanan yang dapat di exploit. Pengertian exploit sangat populer di kalangan Hacker dan banyak sekali ragam exploit yang dapat dimanfaatkan. Exploit dimanfaatkan karena adanya kelemahan (vulnerabilities). Kelemahan-kelemahan yang vatal pada umunya terdapat pada "daemon". Daemon adalah suatu komputer yang memberikan service pada jaringan/internet. Misalnya komputer yang memberikan service telnet disebut sebagai telnet daemon (telnetd), yang memberikan service File Tranfer Protocol (FTP) disebut ftpd. Dan seterusnya. Setiap sistem memiliki kelemahan (vulnerabilities) dan kelemahan ini dapat dimanfaatkan (dieksploitasi) oleh yang memahaminya. Dari sinilah timbul istilah exploit, yakni suatu skrip atau program kecil yang khusus diciptakan untuk mengekploitasi kelemahan.

Teknologi komunikasi dan informasi tidak terbatas pada ilmu komputer saja. Pada dasarnya secara umum orang akan menyebut sebagai teknologi

informasi saja atau TI. Yang tergabung dalam TI secara umum adalah Komputer, Telepon, Televisi dan satelit, bahkan kini sudah termasuk aliran listrik sebagai media TI, karena power line (jalur listrik) sudah dimanfaatkan sebagai media menghantar data, misalnya pada teknologi Power Line Communication (PLC) yang dikembangkan oleh PLN, dan suatu saat nanti PLN akan berkembang menjadi Power Line Network, yakni PLN2PLN.

Semua unsur TI dapat dijadikan sarana teror oleh teroris, tergantung dari tingkat kemahirannya, apakah akan mengacak jalur satelit, pasokan listrik, air, peluru kendali, sistem perbankan, penerbangan, kelautan, televisi, radio, dsb. Apapun targetnya, tetap akan menggunakan komputer dan jaringannya serta koneksi globalnya untuk mencapai target. Jadi inti TI nya di sini adalah pada sistem komputer dan jaringannya serta koneksi ke jaringan global.

Timbul pertanyaan, jika demikian TI tidak akan pernah aman 100 % ? itu sangat betul. Karena tidak ada sistem yang bisa aman 100%, akan selalu ada celah kelemahan. Cara yang paling aman adalah, putuskan hubungan modem, putuskan kabe-kabel jaringan, tutup koneksi ke internet, buang Monitor, Keyboard dan CPU dan kembali beralih ke masin ketik. Dengan demikian kita akan kembali ke peradaban yang primitif dengan berbagai tingkat kesulitan yang jauh melebihi dari sekadar IT Security.

## KEGIATAN TERORISME SEBAGAI DAMPAK DARI TEKNOLOGI KOMUNIKASI DAN INFORMASI:

Terorisme pada dasarnya sudah terjadi, jika seseorang atau sekelompok orang telah melakukan kegiatan illegal melalui teknologi informasi. Misalnya, seorang penyusup masuk ke sistem komputer yang diproteksi milik pihak lain dan mencuri data atau merusak data maupun informasi. Kegiatan ini sudah masuk dalam kategori "teroris informasi", karena prilakunya sudah meresahkan pihak lain dan berpotensi merugikan masyarakat. Kegiatan-kegiatan terorisme dengan menggunakan teknologi komunikasi dan informasi, dapat dilakukan dalam bentuk :

CARDING : yaitu memanfaatkan kartu kredit orang lain untuk berbelanja di toko-toko online, guna membeli bahan peledak, senjata, atau dalam upaya pengumpulan dana. Carding tidak dikenal dalam tata bahasa Inggris, namun istilah ini lahir dari pemakaian istilah baru dalam dunia internet. Istilah yang paling tepat adalah Credit Card Fraud. Di sini teroris akan mencari nomor-nomor Credit Card (CC) orang lain melalui chanel di IRC, melalui CC Generator, meng-hack toko online dan masuk ke database-nya, membuat wesite palsu tentang validasi kartu kredit seperti yang umum ada di situs-situs porno.

e-MAIL: fasilitas ini dapat dimafaatkan teroris untuk berkomunikasi keseluruh dunia untuk kegiatan kelompoknya. Dengan e-mail sangat murah, mudah, cepat, tepat, akurat, dan praktis. Fasilitas e-mail dapat juga digunakan untuk menteror pihak lain dalam bentuk ancaman-ancaman, penekanan, pemerasan, penipuan, spamming dan untuk menyebar virus ganas yang fatal.

MEMBAJAK MEDIA:

Kelompok teroris dapat membajak media dengan "menunggangi" satelit dan siaran-siaran TV Kabel untuk menyiarkan pesan-pesan organisasi mereka. Alat yang umum digunakan adalah *antenna parabola* yang sudah dimodifikasi agar dapat memancarkan sinyal ke satelit dan saluran TV Kabel yang dituju. Contoh kasus pembajak media yang cukup terkenal adalah kasus "Captain Midnight", seorang pembajak media dari Dallas, Texas USA yang pada tahun 1986 memanipulasi siaran HBO yang berjudul " The Falcon and the Snowman" untuk menampilkan pesan-pesan pribadinya. Selain memanipulasi sinyal TV Kabel, mereka juga mencari metoda-metoda untuk membongkar "penyandian" sinyal-sinyal TV Kabel yang telah ada untuk kemudian menyadap siarannya.

PHREAKER:

Phreaker sering dijabarkan sebagai Phone fREAKER, adalah kelompok yang berusaha mempelajari dan menjelajahi segala aspek dalam sistem telepon. Pada awalnya sistem telepon seperti di Amerika masih dikendalikan oleh nada-nada berfrekuensi tinggi *(Sistem Multy Frequency)*. Dan sistem ini telah dapat diakali oleh para phreaker dan mengendalikannya.

Setelah perusahaan-perusahaan telekomunikasi di Amerika menggunakan komputer untuk mengendalikan jaringan telepon, para phreaker juga beralih ke komputer dan menjadi mirip seperti Hacker. Para phreaker mempelajari tehnik komputer agar bisa melanjutkan penjelajahannya pada jaringan telepon yang kini dikendalikan oleh komputer. Demikian juga sebaliknya, dan para Hacker mempelajari teknik phreaking agar dapat memanipulasi sistem telepon untuk menekan biaya-biaya sambungan telepon, dan untuk menghindari pelacakan.

LAIN-LAIN:

Kasus lainnya adalah di Amerika, pada bulan April dan Mei 2002 di California, telah terjadi gangguan aliran listrik, sehingga wilayah tersebut kehilangan pasokan tenaga listrik secara total, akibat serangan Hacker dari China. Di

Jepang Tahun ..? telah terjadi hacking pada sistem penerbangan sipil yang telah mengacaukan sistem komputer pada bandara Nagoya yang hampir merenggut korban jiwa.

Selain cara-cara di atas, masih ada cara-cara lain yang dapat digunakan oleh teroris, misalnya : Wiretapping, Hacking, Cybersquatters, Virus Attack, DoS. Defacing, Domain Hijacking, Treespassing, illegal acces, illegal Interception, Data Interference, System Interference, Cyberpornography, dan lain-lainnya yang tidak mungkin dijelaskan satu-persatu.

HACKING UNTUK MERUSAK SISTEM :

Aktivitas seorang hacker secara garis besar dapat dibagi menjadi 4, tahapan, yakni:

- Mencari Sistem komputer dan mengumpulkan informasi, untuk dimasuki.
- Menyusup Masuk
- Menjelajahi sistem tersebut dan mencari akses ke seluruh bagian.
- Membuat backdoor dan menghilangkan jejak.

Dari seluruh kegiatan ini, teroris dapat melakukan apa saja sesuai dengan maksud dan tujuannya yang ditargetkan kepada infrastruktur strategis yang vital.

Secara sederhana dapat digambarkan bahwa kegiatan teroris melalui fasilitas teknologi komunikasi dan informasi dapat digambarkan dengan kegiatan-kegiatan sebagai berikut:

FOOT PRINTING : Adalah kegiatan mencari sistem komputer. Kegiatan ini adalah suatu usaha untuk mencari informasi lewat proses "non-intrusif" Tidak semua infrastruktur strategis yang vital terhubung ke jaringan global. Hacker teroris dapat dipastikan akan mencari sistem dengan cara menghubungi nomor-nomor telepon yang dicurigai terhubung ke jaringan dengan modem. Nomor-nomor telepon tersebut dihubungi oleh teroris dengan maksud untuk mendapatkan "sinyal carrier" (terhubung ke modem komputer). Cara ini bisa manual bisa dengan program khusus yakni "prefix scanner", Demon Dialer atau War Dialer, contoh programnya adalah : Tone Lock. Akan tetapi, jika suatu komputer/jaringan sudah terhubung ke jaringan global internet lebih gampang daripada cara di atas, yakni bukan komputernya yang dicari tetapi "pintu masuk" yang dapat dimanfaatkan dalam sistem komputer.

SCANNING : Yaitu kegiatan untuk mencari pintu masuk. Pintu masuk ini berupa "Port" yaitu jalur keluar - masuknya data dari dan ke suatu komputer.

Pengaksesan melalui port ini disebut "port surfing". Pencarian port ini dapat dilakukan dengan port scanner seperti Rebillion, Port Pro dan Port Scanner guna memeriksa alamat IP untuk mencari port yang terbuka seperti port 23 (telnet), 43 (whois), 79 (finger), 29 (SMTP) dan seterusnya.

ENUMERATION:

Enumeration adalah kegiatan berupa langkah-langkah yang perlu dilakukan seorang hacker untuk mengumpulkan informasi mengenai sasaran yang akan ditujunya. Proses enumaration ini bersifat spesifik berdasarkan sistem operasi yang dipakai oleh target/calon korban. Enumerasi adalah proses pencarian informasi lebih lanjut untuk mematangkan serangan. Perbedaan enumerasi dengan kedua proses terdahulu adalah pada "tingkat intrusinya", yang mengharuskan hacker harus log in ke sasaran. Informasi yang dikumpulkan, misalnya pada sistem Windows NT/200 yang sangat spesifik pada sasaran yang dituju adalah: Network resource dan share, User dan group, serta Aplikasi dan banner. Sepintas informasi yang dikumpulkan tidak berbahaya, namun informasi yang bocor dan lubang-lubang ini dapat menjadi awal serangan hacking. Hacker akrab mencari user name yang absah dan masuk dengan menebak password user name tersebut yang kemudian terhubung ke kelemahan pada *protocol resorce sharing*. Protokol ini merupakan tempat awal hacker untuk menjejakkan kakinya di sistem korban.

CREATING BACKDOOR:

Backdoor pada prinsipnya adalah "jalan tembus" yang dibuat hacker setelah masuk, yang berguna untuk kembali tanpa perlu melalui sistemteksi lagi. Backdoor dibuat berdasarkan spesifikasi dari sistem sasaran yang dipakai. Kegiatan membuat backdoor ini bersamaan dengan usaha untuk menghilangkan jejak. Salah satu cara yang paling umum adalah dengan meng-edit file-file log pada sistem yang dimasuki, dan menghilangkan semua entry yang berhubungan dengan din si hacker. Salah satu cara menyamarkan identitas, misalnya dengan *"bouncing"*, yakni memanfaatkan suatu sistem sebagai basis operasi untuk memasuki operasi lain. Dalam praktek bouncing, jejak-jejak akan mengarah ke komputer yang akan dijadikan basis operasi dan bukan ke lokasi hacker yang sebanarnya. Manfaat bouncing selain untuk menyulitkan pelacakan, sebenarnya juga untuk melewati berbagai program proteksi. Misalnya: komputer A (Web Server) dan Komputer B (FTP Server) berada dalam jaringan/subnet yang terhubung ke internet. A diproteksi dengan "firewall". Maka hacker yang ingin masuk ke komputer /dapat memerintahkan

komputer B (yang terbuka untuk umum) untuk melakukan koneksi ke port tertentu di A. Koneksi ini dapat dimanfaatkan oleh Hacker karena.B dan A berada dalam suatu subnet yang sama, maka lalu lintas data yang terjadi tidak akan disaring oleh program Firewall, karena firewall hanya menyaring paket data dari luar subnet saja.

STRATEGI PENANGANAN:

1. MEMBENTUK CYBER TASK FORCE

Satuan yang terintegrasi dan berkemampuan "Quick Response" di Mabes Polri & Kewilayahan. Di Jepang cyber taskforce didirikan April 2001, dirancang untuk menghadapi aspek-aspek tehnis respon darurat bila serangan cyber-teroris terjadi. Ada pada setiap Polda. Cyber- Task Force Center ada pada Markas Besar Kepolisian dan kewilayahan, yang berperan antara lain : •Pusat komando & informasi•Membangun hubungan kerja yang baik dengan infrastruktur kritis•Mengumpulkan/menganalisa informasi -Merespon segera situasi darurat untuk memperkecil kerusakan• Intrusion Detection System.

Misinya dari Cyber Task Force adalah: mencegah serta merespon keadaan darurat agar kerugian / resiko akibat serangan pada Sistem Informasi terhadap infra struktur kritis seminimal mungkin, dengan kegiatan antara lain; Assess kerawanan dari infrastruktur kritis, merespon secara cepat keadaan darurat agar kerusakan diharapkan seminimal mungkin, dan menyediakan bimbingan dan bantuan investigasi.

2. MEMASANG REAL TIME INTRUSION DETECTION SYSTEM

Sistem early warning & Quick response dari Interdep dan Organisasi IT "Yang secara cepat dengan waktu sebenarnya mendeteksi terjadinya gangguan"

(Adaposi dari Cyber Terorism Technology Office, NPA).3. MEMBENTUK TIM KOORDINASI PERLINDUNGAN KEAMANAN DAN PENANGGULANGAN INFRASTRUKTUR STRATEGIS BERBASIS TEKNOLOGI INFORMASI.

Tim koordinasi ini beranggotakan unsur-unsur dari Kepolisian RI, Kominfo, Dep. Pertahanan, Badan Intelejen Negara, Badan Standarisasi Nasional, Lembaga Sandi Negara, Ditjen Postel Dephub, Kejaksaan dan Departemen Kehakiman dan HAM, Perguruan Tinggi, Assosiasi dan LSM. Dari Tim Koordinasi ini akan dibentuk Task Force IT Security yang tujuannya untuk memberikan perlindungan dan respon cepat terhadap kejahatan-kejahatan berbasis teknologi informasi. Di samping itu sebagai dasar acuan kerja dengan

pihak Kepolisian negara, Kominfo telah membuat nota kesepakatan (Memory of Understanding) bersama-sama dengan pihak Polri.

4. MEMBEKTUK CYBER PATROL:

Secara garis besar Cyber Patrol direncanakan akan memiliki peran-peran sebagai berikut:

a. Standar Nasional Keamanan TI. yang mencakup di dalamnya seperti; Membangun standar dan penyebaran sistem IT Security, Mencegah cyber crime, cyber patrol menyediakan berbagai tindakan keamanan, dan Membentuk unit Anti Cyber crime.

b. Layanan IDS; seperti :
   - Mengaudit kerentanan sistem e-government nasional
   - Melawan/menangkal berbagai tipe serangan Cyber
   - Audit, deteksi, dan menangkal penyusup.

c. Keamanan Info-Structures:
   - Info struktur termasuk kebijakannya, aturannya, keamanan organisasi, dan teknisi cyber patrol skillful
   - System alone tidak dilayani oleh cyber patrol
   - Unit Penelitian dan Pembangunan (Litbang).

Dalam Cyber Patrol, yang paling menonjol adalah ada empat hal, yakni: Intrusion Detectuion System, Integrity Protection System, Access Control System, dan Post-even Analysis System. Dari keempat sistem tersebut, semua terintegritas dalam system cyber patrol, dan berfungsi sebagai protector terhadap infrastruktur strategis yang vital serta mengolah permintaan-permintaan audit kerentanan oleh jaringan/infrastruktur pemerintahan baik yang ada di pusat maupun di daerah maupun ke infrastruktur yang terhubung lainnya.

5. MEMBUAT PERATURAN PERUNDANG-UNDANGAN TENTANG TINDAK PIDANA YANG BERBASIS TEKNOLOGI INFORMASI

Pemerintah sejogianya memperhatikan aspek-aspek legal dalam tindak pidana yang berbasis teknologi informasi. Misalnya menyempurnakan Undang-Undang Anti Teroris dengan memasukkan klausula-klausula tindak pidana atau kegiatan terorisme yang difasilitasi dengan teknologi komunikasi dan informasi dan mendefinisikannya lebih tegas. Selain itu, dapat pula dilakukan cara-cara lain guna mengantisipasi kejahatan-kejahatan di dunia maya, seperti

misalnya : •Menghapuskan pasal-pasal dalam UU terkait yang tidak terpakai lagi (usang); •Mengamandemen KUHP; •Mensisipkan hasil kajian dalam RUU yang ada, (RUU Informasi dan Transaksi Elektronik) •Membuat RUU tersediri, (RUU Tindak Pidana Teknologi Informasi).

PENUTUP:

Teknologi komunikasi dan informasi atau yang lazim dikenal sebagai ICT (Information Communication Technology) memiliki sisi terang dan sisi gelap. Salah satu sisi gelap dan dampak teknologi komunikasi dan informasi adalah dipakai untuk kegiatan terorisme. Kegiatan terorisme yang difasilitasi oleh teknologi komunikasi dan informasi merupakan bagian dan kejahatan berbasis teknologi informasi. Perbedaannya hanya pada motifnya, sasaran, tujuan dan dampak yang ditimbulkannya. Banyak cara yang dapat digunakan oleh teroris dalam melaksanakan aksinya di dunia cyber, sesuai dengan tujuan dan kemampuan tehnis teroris yang dimiliki serta tersedianya lubang-lubang keamanan yang dapat dijadikan jalan masuk ke dalam infrastruktur yang akan dijadikan sasaran sebagai sarana teror.

Di Indonesia belum ada kasus yang menonjol kegiatan terorisme di dunia maya. Akan tetapi dikemudian hari, bukanlah mustahil teror dapat dilakukan melalui teknologi komunikasi dan informasi dengan merusak dan mengacaukan infrastruktur-infrastruktur strategi yang vital yang berpotensi memiliki berdampak politis, ekonomis, keamanan dan pertahanan bagi hajat hidup rakyat banyak.

Untuk mewaspadai potensi bahaya terorisme di dunia cyber, pemerintah telah membentuk Cyber Task Force di Mabes Polri dan jajarannya, membentuk Task Force IT Security Nasional, membentuk Cyber Patrol,dan membentuk Tim Kordinasi Perlindungan Keamanan dan Penaggulangan Infrastruktur Strategis Berbasis Teknologi Informasi. Dari keseluruhan sistem pengamanan ini diharapkan akan terjadi sinergi dalam dunia TI secara nasional, regional dan internasional guna mencegah dan menanggulangi kejehatan-kejahatan yang berbasis teknologi informasi.