APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

MANAJEMEN KEAMANAN INFORMASI DAN INTERNET

Topik Bahasan

CYBER 6: FENOMENA KEAMANAN INFORMASI DALAM DUNIA SIBER

Versi

2013/1.0

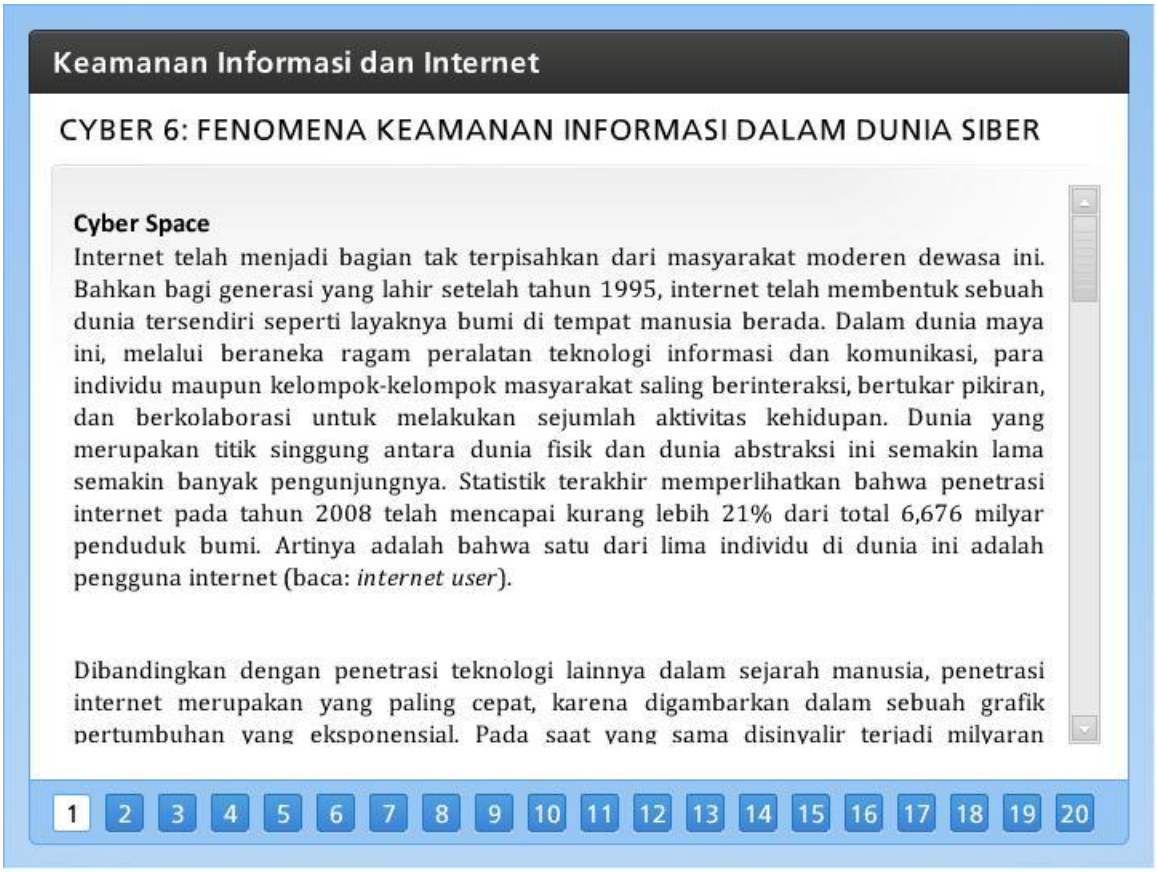
Nama File

MKIDI-1A-FenomenaKeamanan.pdf

Referensi Pembelajaran

1-A

CYBER 6: FENOMENA KEAMANAN INFORMASI DALAM DUNIA SIBER



Cyber Space

Internet telah menjadi bagian tak terpisahkan dari masyarakat moderen dewasa ini. Bahkan bagi generasi yang lahir setelah tahun 1995, internet telah membentuk sebuah dunia tersendiri seperti layaknya bumi di tempat manusia berada. Dalam dunia maya ini, melalui beraneka ragam peralatan teknologi informasi dan komunikasi, para individu maupun kelompok-kelompok masyarakat saling berinteraksi, bertukar pikiran, dan berkolaborasi untuk melakukan sejumlah aktivitas kehidupan. Dunia yang merupakan titik singgung antara dunia fisik dan dunia abstraksi ini semakin lama semakin banyak pengunjungnya. Statistik terakhir memperlihatkan bahwa penetrasi internet pada tahun 2008 telah mencapai kurang lebih 21% dari total 6,676 milyar penduduk bumi. Artinya adalah bahwa satu dari lima individu di dunia ini adalah pengguna internet (baca: *internet user*).

Dibandingkan dengan penetrasi teknologi lainnya dalam sejarah manusia, penetrasi internet merupakan yang paling cepat, karena digambarkan dalam sebuah grafik pertumbuhan yang eksponensial. Pada saat yang sama disinyalir terjadi milyaran transaksi per hari dengan nilai

transaksi mencapai milyaran dolar Amerika per detiknya - terjadi tanpa henti selama 24 jam sehari dan 7 hari seminggu. Suatu frekuensi dan volume perdangangan yang belum pernah sebelumya terjadi dalam sejarah kehidupan manusia. Semua fakta ini mengandung arti bahwa domain "pasar" yang terbentuk di internet memiliki nilai atau *value* yang sedemikian tingginya, karena lambat laun semakin banyak transaksi dan interaksi yang terjadi di sana. Bahkan sejumlah sumber mensinyalir, dalam waktu yang tidak lama lagi, nilai perdagangan di internet akan menjadi jauh lebih besar daripada yang terjadi di dunia nyata. Singkat kata, internet merupakan sebuah entitas yang tidak ternilai harganya - yang dari masa ke masa, akan semakin meningkat harga dan nilainya, karena semakin banyak aktivitas yang terjadi di sana.

Cyber Threat

Sebagaimana adanya sebuah benda berharga, pasti diiringi pula dengan banyaknya pihak yang tertarik untuk "memilikinya". Perhiasan misalnya, sering kali diburu orang untuk dijadikan milik karena nilainya yang makin lama makin meningkat (baca: investasi berharga). Namun ada pula pihak-pihak yang ingin memilikinya dengan cara-cara yang jahat, seperti ingin mencurinya, merampok, bahkan merebutnya dari kepemilikan yang sah. Demikian pula hal yang sama menimpa internet. Semakin bertambah nilai dunia maya ini, semakin banyak pula ancaman yang menyertainya.

Ancaman pertama berupa keinginan sejumlah atau sekelompok orang maupun pihak yang ingin mengambil beraneka ragam harta atau barang berharga yang ditransaksikan atau dipertukarkan di internet. Mulai dari hal-hal yang secara langsung merepresentasikan sumber daya finansial, seperti uang digital, nilai kartu debit, kekayaan di rekening bank, jumlah tagihan kartu kredit, dan lain sebagainya - hingga entitas *intangible* yang memiliki nilai strategis tertentu seperti data intelijen, *password* rekening bank, informasi rahasia konsumen, dan lain-lain.

Ancaman kedua berupa niat orang-orang jahat tersebut untuk membuat agar internet tidak berfungsi secara normal, atau dengan kata lain mencoba membuat terjadinya mal fungsi pada internet. Harapannya adalah agar terjadi gangguan pada proses transaksi perdagangan, aktivitas akses informasi, prosedur administrasi pemerintahan, dan lain sebagainya. Karena semakin banyak aspek kehidupan yang tergantung pada internet, maka gangguan ini dapat mengakibatkan terjadinya *chaos* yang berkepanjangan.

Ancaman ketiga berupa usaha melakukan modifikasi terhadap data atau informasi yang mengalir di internet demi tujuan-tujuan destruktif, seperti memfitnah, menyesatkan, mengadu domba, menghancurkan citra, menipu, dan lain-lain. Bagi bangsa-bangsa yang secara fisik maupun ideologis masih berperang, cara-cara tersebut di atas merupakan aktivitas "perang" sehari-hari yang dapat terjadi di dunia maya.

Ancaman keempat berupa kehendak individu untuk menyebarkan hal-hal yang keliru ke seluruh penduduk di dunia, seperti: faham-faham yang menyesatkan, citra dan media pornografi, informasi pendukung tindakan terorisme, tawaran aktivitas perjudian, cara-cara melakukan kejahatan terselubung, dan lain sebagainya.

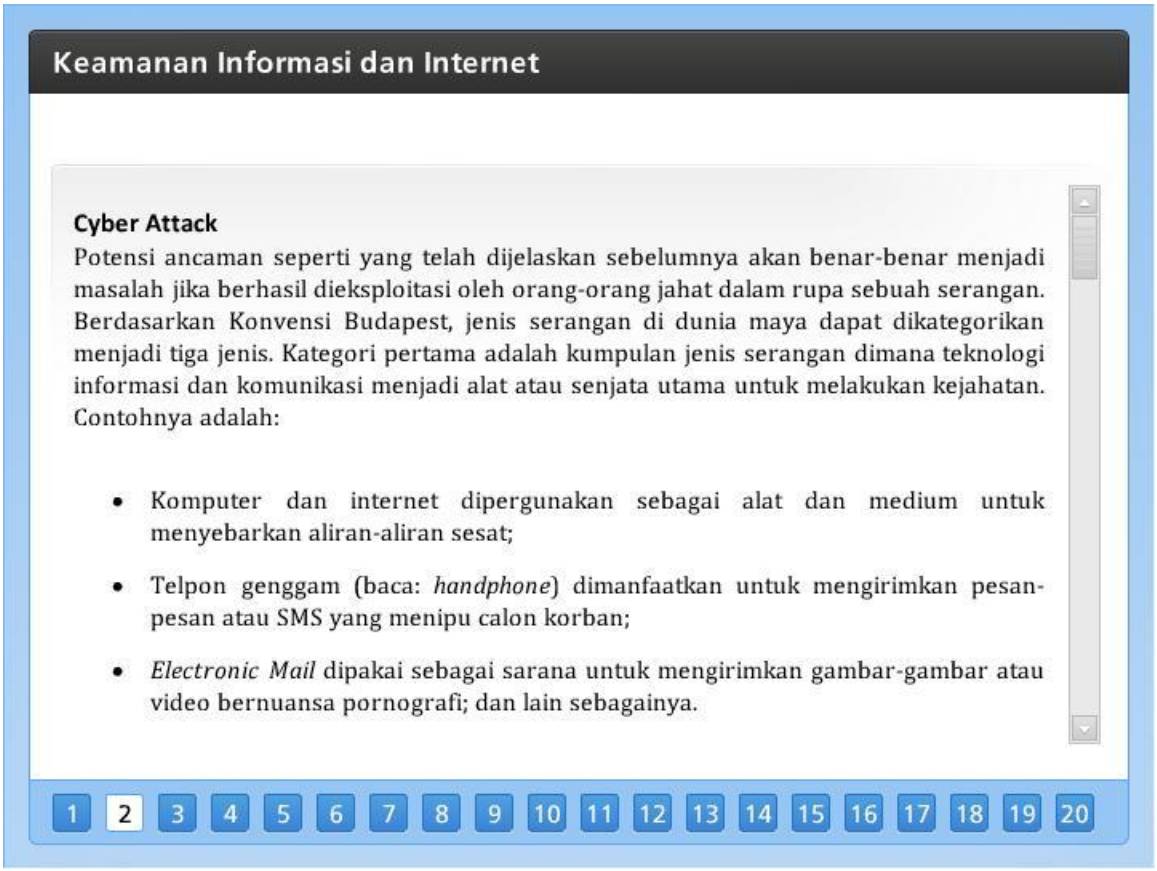
Ancaman kelima atau terakhir berupa penyebaran dan penanaman program-program jahat (baca: *malicious software*) ke komputer-komputer yang terhubung ke internet dengan tujuan yang berane-ragam, mulai dari yang bersifat non-destruktif - seperti adanya tampilan yang tidak diiginkan, mengacaukan fungsi huruf pada papan tekan (baca: *keyboard*), tidak bekerjanya peralatan input-output, dan lain-lain - hingga yang bersifat sangat destruktif, seperti menghapus isi pada *hard disk*, mengambil data tanpa sepengetahuan pemilik, memata-matai aktivitas pengguna, memacetkan komputer atau lebih dikenal dengan istilah "hang", menurunkan kinerja kecepatan prosesor, dan hal-hal lain yang sangat merugikan.

Informasi berikut memperlihatkan bagaimana mengerikannya ancaman yang ada di dunia maya saat ini. Sebagai contoh, ada sebuah situs yang menjual 29,000 alamat email individu dengan harga 5 dolar Amerika; sementara ada situs lain yang hanya dengan uang US$ 300 dapat memberikan informasi terkait dengan rekening bank individu yang memiliki uang di atas 100 juta rupiah; atau sebuah situs yang menawarkan jasa merusak situs (baca: *website*) dengan kisaran tarif tiga hingga lima dolar per situsnya.

Keseluruhan ancaman atau *threat* ini merupakan hal yang wajar karena tingginya nilai internet seperti yang dijelaskan sebelumnya. Oleh karena itu, siapapun pengguna internet, hendaklah waspada dan berhati-hati terhadap resiko ancaman yang menyertainya.

Disamping itu, tidak ada teknologi informasi yang didesain secara sempurna sehingga bebas dari kerawanan (baca: *vulnerabilities*). Laporan dari berbagai lembaga riset dan pengawas internet memperlihatkan bahwa kerawanan pada program aplikasi (baca: *software*) semakin

lama semakin bertambah kuantitas dan kualitasnya. Hal ini sejalan dengan semakin banyak dan kompleksnya jumlah *incident* yang terjadi di dunia maya akibat eksploitasi terhadap kerawanan tersebut oleh pihak-pihak yang tidak bertanggung jawab. Singkat kata, sejalan dengan bermanfaatnya aplikasi teknologi informasi bagi umat manusia, bertambah pula resiko intrinsik yang terkandung di dalamnya (baca: *embedded risk*). Melakukan mitigasi terhadap resiko tersebut - dalam arti kata mengurangi tingginya probabilitas terjadinya eksploitasi pada ancaman tersebut, atau paling tidak mengurangi dampak kerugian yang diakibatkan oleh *incident* yang tak terindahkan - merupakan hal bijaksana yang dapat dilakukan oleh semua orang.



Cyber Attack

Potensi ancaman seperti yang telah dijelaskan sebelumnya akan benar-benar menjadi masalah jika berhasil dieksploitasi oleh orang-orang jahat dalam rupa sebuah serangan. Berdasarkan Konvensi Budapest, jenis serangan di dunia maya dapat dikategorikan menjadi tiga jenis. Kategori pertama adalah kumpulan jenis serangan dimana teknologi informasi dan komunikasi menjadi alat atau senjata utama untuk melakukan kejahatan. Contohnya adalah:

- Komputer dan internet dipergunakan sebagai alat dan medium untuk menyebarkan aliran-aliran sesat;
- Telpon genggam (baca: *handphone*) dimanfaatkan untuk mengirimkan pesan-pesan atau SMS yang menipu calon korban;
- *Electronic Mail* dipakai sebagai sarana untuk mengirimkan gambar-gambar atau video bernuansa pornografi; dan lain sebagainya.

Kategori kedua adalah kumpulan peristiwa dimana komputer atau teknologi informasi menjadi sasaran pusat serangan dari pelaku tindak kejahatan, seperti:

- Melakukan transaksi keuangan fiktif dalam sebuah sistem perbankan berbasis internet (baca: *e-banking*);
- Mematikan atau memacetkan kerja sebuah jejaring internet (baca: *LAN* atau *WAN*) secara *remote*;
- Menyebarkan virus-virus untuk mengganggu kinerja komputer-komputer tertentu; dan lain sebagainya.

Adapun kategori jenis serangan ketiga ditujukan bagi peristiwa yang bertujuan utama untuk merusak (termasuk memodifikasi dan memfabrikasinya) data atau informasi yang tersimpan di dalam media perangkat teknologi informasi. Serangan yang dimaksud antara lain:

- Merubah isi sebuah situs tanpa sepengetahuan pemiliknya;
- Mengambil kumpulan *password* atau informasi lengkap kartu kredit sekelompok individu untuk disalahgunakan atau diperjualbelikan;
- Merusak sistem basis data utama sehingga semua informasi di dalamnya menjadi tidak dapat terbaca atau diakses secara normal; dan lain sebagainya.

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

Cyber Crime

Sejalan dengan kemajuan teknologi komunikasi dan informasi, semakin kompleks pula jenis serangan yang terjadi di dunia maya. Jika dahulu diperkenalkan istilah *hacker*dan *cracker* yang menunjuk pada individu dengan kemampuan dan aktivitas khusus memasuki sistem komputer lain untuk beraneka ragam tujuan, maka saat ini sudah banyak diciptakan mesin atau sistem yang dapat bekerja sendiri secara intelijen untuk melakukan teknik-teknik penyusupan dan perusakan sistem. Intinya adalah bahwa serangan terhadap sistem keamanan teknologi informasi organisasi telah masuk pada kategori kriminal, baik yang bersifat pidana maupun perdata. Walaupun kebanyakan jenis tindakan kriminal tersebut berkaitan erat dengan urusan finansial, tidak jarang akibat serangan tersebut, sejumlah nyawa manusia melayang, karena menimpa sistem yang sangat vital bagi kehidupan manusia. Ilustrasi berikut memperlihatkan begitu banyaknya jenis tindakan atau serangan yang mengarah pada kriminalisasi dari tahun ke tahun.

dari semakin beraneka ragamnya jenis serangan yang ada, secara prinsip terdapat 4 (empat) jenis aktivitas yang kerap dikategorisasikan sebagai tindakan kriminal dalam dunia teknologi informasi. Pertama adalah *interception*, yaitu tindakan menyadap transmisi yang terjadi antara satu pihak dengan pihak yang lain. Seperti diketahui, di Indonesia misalnya, hanya sejumlah lembaga yang memiliki hak untuk melakukan penyadapan atau intersepsi, seperti Kepolisian Republik Indonesia, Badan Intelijen Nasional, dan Komisi Pemberantasan Korupsi. Individu atau organisasi yang tidak memiliki wewenang untuk melakukan hal tersebut dapat diadili jika melakukan tindakan terkait dengan penyadapan. Kedua adalah *interruption*, yaitu tindakan yang mengakibatkan terjadinya pemutusan komunikasi antara dua buah pihak yang seharusnya berinteraksi. Fenomena *Denial of Services (DoS)* atau *Distributed Denial of Services (DDoS)* merupakan salah satu serangan yang dapat mengakibatkan terjadinya kondisi interupsi pada sistem komputer. Ketiga adalah *modification*, yaitu tindakan melakukan perubahan terhadap data atau informasi atau konten yang mengalir dalam sebuah infrastruktur teknologi informasi tanpa sepengetahuan yang mengirimkan/menerimanya. *Web defacement*merupakan salah satu jenis serangan yang bisa dikategorikan dalam kelas ini. Dan yang keempat adalah *fabrication*, yaitu tindakan mengelabui seolah-olah terjadi suatu permintaan interaksi dari seseorang seperti yang dewasa ini dikenal dengan istiliah *phishing*.

Studi mendalam mengenai tindakan kriminal di dunia maya memperlihatkan berbagai motif atau alasan seseorang melakukannya, mulai dari mencari sensasi semata hingga dibiayai oleh sekelompok sponsor teroris internasional. Hampir seluruh negara melaporkan bahwa tindakan kriminal di dunia maya menunjukkan pertumbuhan yang semakin signifikan, baik dilihat dari sisi kuantitas maupun kualitasnya.

Cyber Law

Pada akhirnya, *cyber security* semata tidak dapat mencegah terjadinya motif kriminal di dunia maya, perlu perangkat lain yang lebih canggih dan efektif. Dalam kaitan inilah maka beberapa negara mulai menyusun dan memberlakukan undang-undang dunia maya (baca: *cyber law*). Dalam undang-undang ini biasanya disusun berbagai jenis klasifikasi dan ancaman hukuman terhadap beraneka ragam tindakan kriminal terkait dengan dunia komputer dan/atau teknologi informasi. Walaupun relatif terlambat dibandingkan dengan negara lain, pada akhirnya Indonesia memiliki undang-undang *cyber law*pertamanya yang disusun oleh Departemen Komunikasi dan Informatika dan disetujui oleh Dewan Perwakilan Rakyat untuk mulai diundangkan semenjak tanggal 25 Maret 2008. Undang-undang no.11 tahun 2008 ini dikenal dengan nama Undang-Undang ITE atau Undang-Undang Informasi dan Transaksi Elektronik. Dengan diberlakukannya undang-undang ini, maka berbagai jenis tindakan kriminal di dunia maya dapat dikenakan sanksi tegas secara perdata maupun pidana.

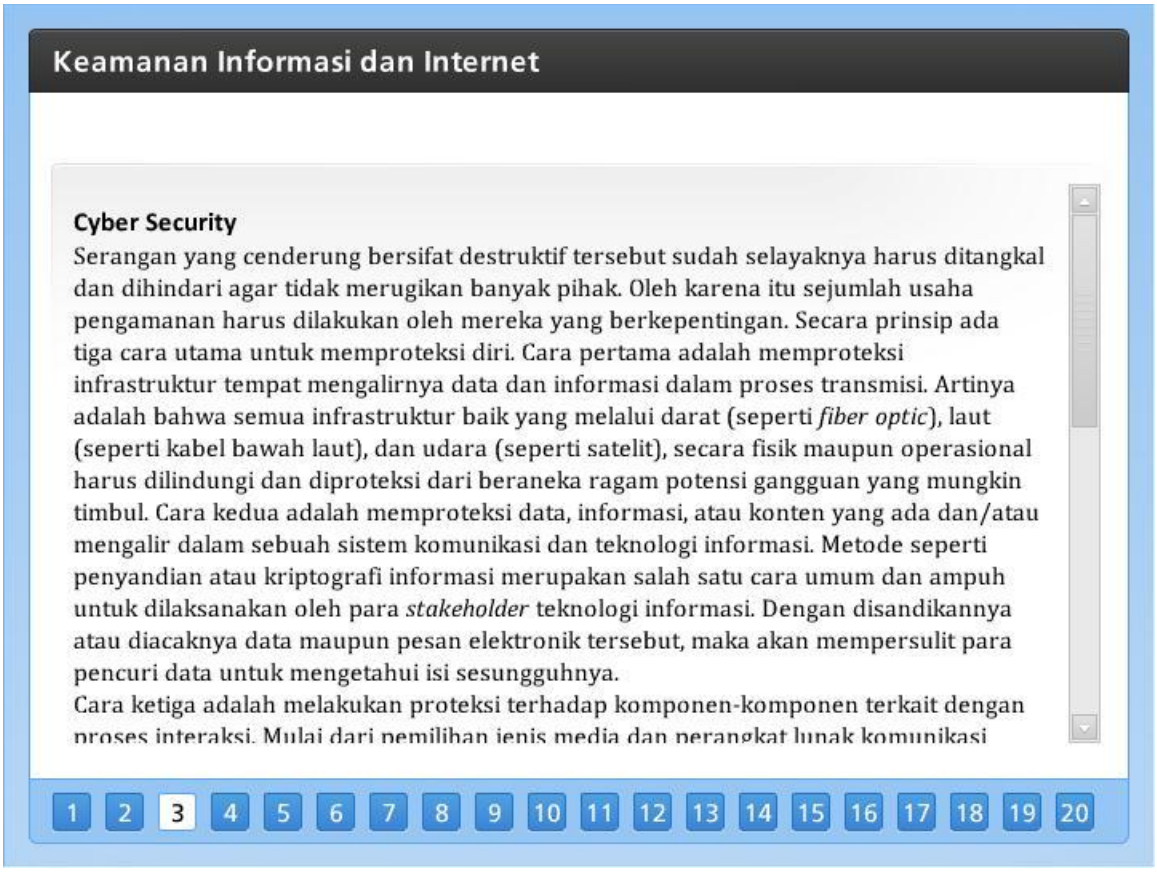
Terlepas dari telah berlakunya undang-undang tersebut, hal yang merupakan tantangan utama adalah implementasinya. Terutama dilihat dari kesiapan sumber daya penegak hukumnya. Sistem hukum di Indonesia menuntut agar polisi, jaksa, pengacara, dan hakim dipersenjatai dengan pengetahuan yang cukup di bidang teknologi informasi agar dapat menghadapi beraneka ragam jenis kasus kriminal di dunia maya. Belum lagi terhitung diperlukannya para saksi ahli di bidang teknologi informasi yang memiliki pengetahuan, kemampuan, kompetensi, dan keahlian terkait dengan keamanan komputer, pengamanan data, forensik alat bukti digital, dan lain sebagainya.

Disamping sumber daya manusia, dibutuhkan pula sejumlah laboratorium dan pusat penelitian di bidang teknologi informasi untuk membantu para penegak hukum dalam menjalankan tugasnya. Keberadaan *Cyber Crime Unit* di Mabes Polri dan *ID-SIRTII* misalnya, dapat membantu

para penegak hukum di Indonesia dalam usahanya untuk melindungi dunia maya dari tangan-tangan jahat.

Pada akhirnya, paradoks antara semakin bernilainya internet akibat manfaat yang ditawarkan kepada khalayak dengan tingginya resiko yang menyertainya, harus dipecahkan dalam tataran filosofis atau pemikiran. Jika tidak, maka keberadaan *cyber security*dan *cyberlaw*misalnya, justru akan menjauhkan orang dari internet - yang tentu saja akan menjadi suatu usaha yang kontra produktif. Bagaimana cara melihat paradoks ini dari kacamata yang lain?

Jika seseorang ditanya, "apakah fungsi sebuah rem bagi kendaraan?" Jawabannya adalah bukan karena ingin agar mobil yang bersangkutan dapat berhenti, namun justru sebaliknya, yaitu agar supir dari mobil yang bersangkutan berani ngebut. Fungsi *cyber security* dan *cyber law*barulah akan efektif jika dengan keberadaannya, justru jumlah pengguna internet di Indonesia meningkat secara signifikan, demikian juga dengan frekuensi dan volume interaksi di internet. Jika dengan keberadaan kedua perangkat tersebut justru membuat pertumbuhan internet menjadi stagnan, berarti banyak hal salah yang perlu untuk diperbaiki.



Cyber Security

Serangan yang cenderung bersifat destruktif tersebut sudah selayaknya harus ditangkal dan dihindari agar tidak merugikan banyak pihak. Oleh karena itu sejumlah usaha pengamanan harus dilakukan oleh mereka yang berkepentingan. Secara prinsip ada tiga cara utama untuk memproteksi diri. Cara pertama adalah memproteksi infrastruktur tempat mengalirnya data dan informasi dalam proses transmisi. Artinya adalah bahwa semua infrastruktur baik yang melalui darat (seperti *fiber optic*), laut (seperti kabel bawah laut), dan udara (seperti satelit), secara fisik maupun operasional harus dilindungi dan diproteksi dari beraneka ragam potensi gangguan yang mungkin timbul. Cara kedua adalah memproteksi data, informasi, atau konten yang ada dan/atau mengalir dalam sebuah sistem komunikasi dan teknologi informasi. Metode seperti penyandian atau kriptografi informasi merupakan salah satu cara umum dan ampuh untuk dilaksanakan oleh para *stakeholder* teknologi informasi. Dengan disandikannya atau diacaknya data maupun pesan elektronik tersebut, maka akan mempersulit para pencuri data untuk mengetahui isi sesungguhnya.

Cara ketiga adalah melakukan proteksi terhadap komponen-komponen terkait dengan proses interaksi. Mulai dari pemilihan jenis media dan perangkat lunak komunikasi *email, chatting, browsing, blogging,* dan lain sebagainya - hingga melakukan *setting* konfigurasi program agar keamanan proses interaksi dapat terjamin dari ancaman. Khusus untuk interaksi yang melibatkan transaksi keuangan misalnya, perlu ditambahkan mekanisme standar pengaman dan prosedur khusus agar tidak terjadi kebocoran dan pencurian data keuangan. Proteksi yang dimaksud, seperti telah disampaikan sebelumnya, adalah dalam rangka mengimplementasikan manajemen resiko atau yang kerap dikatakan sebagai *risk mitigation*.

Dalam kerangka ini terlihat secara jelas, bahwa keberhasilan eksploitasi pada kerawanan teknologi informasi akan mengurangi nilai aset informasi yang dimiliki perusahaan, yang jika tidak diproteksi dengan sistem pengamanan yang memadai serta manajemen kendali yang efektif (baca: kontrol)akan berdampak serius terhadap organisasi terkait.

Banyak orang bertanya-tanya mengenai hal-hal apa saja yang harus diperhatikan dalam rangka mengembangkan sebuah sistem pengamanan yang efektif dan menyeluruh. Standar internasional BS7799/ISO17799 menekankan perlunya memperhatikan 10 (sepuluh) aspek utama untuk memperoleh sistem keamanan yang utuh, holistik, dan menyeluruh. Yang menarik dari standar ini adalah diperhatikannya pula aspek keamanan dalam dunia nyata, dimana

perilaku dan pengetahuan sumber daya manusia menjadi aspek utama yang perlu untuk diperhatikan.