APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

MANAJEMEN KEAMANAN INFORMASI DAN INTERNET

Topik Bahasan

PERANAN KRIPTOLOGI DALAM PENGAMANAN INFORMASI

Versi

2013/1.0

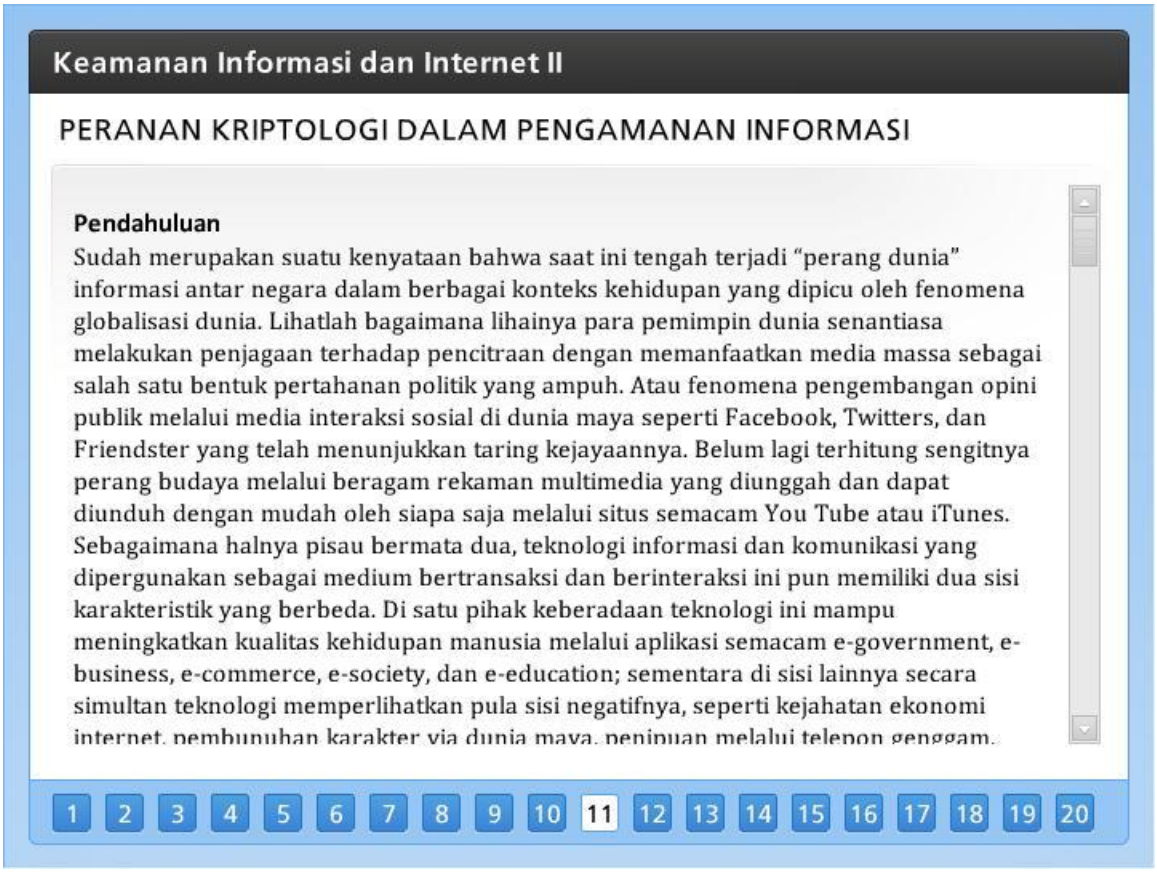
Nama File

MKIDI-9A-PerananKriptologi.pdf

Referensi Pembelajaran

9-A

PERANAN KRIPTOLOGI DALAM PENGAMANAN INFORMASI



Pendahuluan

Sudah merupakan suatu kenyataan bahwa saat ini tengah terjadi "perang dunia" informasi antar negara dalam berbagai konteks kehidupan yang dipicu oleh fenomena globalisasi dunia. Lihatlah bagaimana lihainya para pemimpin dunia senantiasa melakukan penjagaan terhadap pencitraan dengan memanfaatkan media massa sebagai salah satu bentuk pertahanan politik yang ampuh. Atau fenomena pengembangan opini publik melalui media interaksi sosial di dunia maya seperti Facebook, Twitters, dan Friendster yang telah menunjukkan taring kejayaannya. Belum lagi terhitung sengitnya perang budaya melalui beragam rekaman multimedia yang diunggah dan dapat diunduh dengan mudah oleh siapa saja melalui situs semacam You Tube atau iTunes. Sebagaimana halnya pisau bermata dua, teknologi informasi dan komunikasi yang dipergunakan sebagai medium bertransaksi dan berinteraksi ini pun memiliki dua sisi karakteristik yang berbeda. Di satu pihak keberadaan teknologi ini mampu meningkatkan kualitas kehidupan manusia melalui aplikasi semacam e-government, e-business, e-commerce, e-society, dan e-education; sementara di sisi lainnya secara simultan teknologi memperlihatkan pula sisi negatifnya, seperti kejahatan ekonomi internet, pembunuhan karakter via dunia maya,

penipuan melalui telepon genggam, penculikan anak dan remaja lewat situs jejaring sosial, penyadapan terselubung oleh pihak yang tidak berwenang, dan sejumlah hal mengemuka lainnya belakangan ini. Mau tidak mau, suka tidak suka, harus ada suatu usaha dari segenap masyarakat untuk melakukan sesuatu agar dampak teknologi yang positif dapat senantiasa diakselerasi penggunaannya, bersamaan dengan usaha untuk menekan sedapat mungkin pengaruh negatif yang berpotensi berkembang dan berdampak merugikan komunitas luas.

Kejahatan Dunia Maya

Semenjak diperkenalkan dan berkembangnya teknologi internet di penghujung abad 21, statistik memperlihatkan pertumbuhan pengguna teknologi informasi dan komunikasi ini meningkat secara sangat pesat (baca: eksponensial). Pada saat ini diperkirakan 1 dari 5 penduduk dunia telah terhubung ke dunia maya melalui teknologi yang sangat digemari khususnya oleh para generasi muda dewasa ini. Selain sebagai sarana berkomunikasi dan berinteraksi antar berbagai individu maupun beragam kelompok komunitas, internet dipergunakan pula sebagai medium melakukan transaksi dan kolaborasi. Di industri perbankan dan keuangan misalnya, internet dipakai sebagai medium efektif dalam menjalankan transaksi perbankan seperti: transfer uang, lihat saldo, bayar listrik, beli saham, dan lain-lain. Contoh lain adalah di dunia pendidikan, dimana internet dengan variasi teknologi informasi dan komunikasi lainnya dipakai untuk hal-hal semacam: pembelajaran jarak jauh, pencarian referensi belajar, pelaksanaan riset, penyelenggaraan tutorial, dan lain sebagainya. Demikian pula di sektor militer dan pertahanan keamanan, sudah sangat jamak pemanfaatan jejaring internet dan dunia maya untuk melakukan aktivitas seperti: pengiriman pesan rahasia, pemantauan dinamika masyarakat, pengendali peralatan dan fasilitas pertahanan keamanan, penerapan intelijen dan kontera intelijen, dan beragam kegiatan strategis lainnya. Dengan kata lain, pemanfaatan internet serta teknologi informasi dan komunikasi telah masuk ke seluruh aspek kehidupan masyarakat, tanpa terkecual - terutama pada sektor yang sangat vital bagi kelangsungan hidup bermasyarakat dan bernegara, seperti: telekomunikasi, transportasi, distribusi, keuangan, pendidikan, manufaktur, pemerintahan, dan kesehatan.

Seperti halnya pada dunia nyata, dalam dunia nyata pun terjadi berbagai jenis kejahatan yang dilakukan oleh para kriminal dengan beragam latar belakang dan obyektifnya. Statistik memperlihatkan bahwa sejalan dengan perkembangan pengguna internet, meningkat frekuensi terjadinya kejahatan, insiden, dan serangan di dunia maya. Lihatlah beraneka modus operandi yang saat ini tengah menjadi "primadona" sorotan masyarakat seperti:

- penipuan berkedok penyelenggara atau pengelola institusi yang sah melalui SMS, email, chatting, dan website sehingga korban secara tidak sadar mengirimkan atau menyerahkan hak maupun informasi rahasia miliknya (seperti: password, nomor kartu kredit, tanggal lahir, nomor KTP, dan lain sebagainya) kepada pihak kriminal yang selanjutnya nanti dipergunakan untuk merampok harta miliknya via ATM, internet banking, e-comerce, dan lain-lain;
- penyerangan secara intensif dan bertubi-tubi pada fasilitas elektronik milik sebuah institusi - dengan menggunakan virus, botnet, trojan horse, dan program jahat lainnya - sehingga berakibat pada tidak berfungsinya peralatan terkait, dimana pada akhirnya nanti fungsi-fungsi vital seperti perbankan, pasar saham, radar penerbangan, lalu lintas transportas, atau instalasi militer menjadi tidak berfungsi atau pun malfungsi;
- perusakan atau pun perubahan terhadap data atau informasi dengan tujuan jahat seperti memfitnah, merusak citra individu atau institusi, membohongi pihak lain, menakut-nakuti, menyesatkan pengambil keputusan, merintangi transparansi, memutarbalikkan fakta, membentuk persepsi/opini keliru, memanipulasi kebenaran, dan lain sebagainya;
- penanaman program jahat (baca: malicious software) pada komputer-komputer milik korban dengan tujuan memata-matai, menyadap, mencuri data, merubah informasi, merusak piranti, memindai informasi rahasia, dan lain-lain; serta
- penyebaran faham-faham atau pengaruh jahat serta negatif lainnya ke khalayak, terutama yang berkaitan dengan isu pornografi, komunisme, eksploitasi anak, aliran sesat, pembajakan HAKI, terorisme, dan berbagai hal lainnya yang mengancam kedamaian hidup manusia.

Langkah Pengamanan Informasi

Memperhatikan berbagai fenomena ancaman yang ada, reaksi beragam diperlihatkan oleh sejumlah pihak seperti pemerintah, swasta, akademisi, politisi, praktisi, komunitas swadaya, dan kelompok-kelompok masyarakat lainnya. Pada level nasional misalnya, hampir seluruh negara mendirikan apa yang dinamakan sebagai CERT (Computer Emergency Response Team) atau CSIRT (Computer Security Incident Response Team) - sebuah lembaga pengawas dan pengelola insiden berskala nasional jika terjadi serangan pada tingkat nasional. Bahkan di sejumlah negara maju seperti Amerika Serikat dan Jepang, dikembangkan institusi yang sangat berpengaruh dan memegang otoritas tinggi - yang disebut sebagai NSA (National Security Agency) atau NISC (National Information Security Council) - dengan tugas dan tanggung jawab

utama menjaga keamanan informasi pada tataran kenegaraan dan lembaga vital negara yang berpengaruh terhadap kelangsungan hidup masyarakatnya. Di Indonesia institusi serupa bernama ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure).

Pada tataran swasta, proses pengamanan informasi dilakukan pada sektor hulu - yaitu industri telekomunikasi - terutama yang berperan sebagai penyedia jasa penyelenggara koneksi internet (baca: ISP=Internet Service Provider). Berbagai usaha dilakukan oleh perusahaan-perusahaan ini, mulai dari menginstalasi piranti keras seperti sensor, firewalls, Intrusion Prevention System (IPS), dan Intrusion Detection System (IDS), hingga membentuk divisi keamanan internet atau informasi dalam struktur organisasi ISP terkait (baca: internal CERT). Sementara itu tumbuh pula sejumlah perusahaan swasta yang bergerak di bidang jasa konsultasi, pelatihan, dan pendampingan di bidang keamanan informasi.

Sektor pendidikan pun nampak tidak mau kalah berperan. Terbukti dengan mulai ditawarkannya beraneka ragam program, pelatihan, penelitian, seminar, lokakarya, sertifikasi, serta pelayanan dengan kurikulum atau konten utama terkait dengan manajemen keamanan informasi dan internet. Secara serius terlihat bagaimana lembaga pendidikan yang dimotori perguruan tinggi ini berkolaborasi dengan perusahaan swasta berskala nasional, regional, dan internasional dalam menyemaikan kompetensi - terkait dengan ilmu penetration test, malware analysis, ethical hacking, traffic monitoring, secured programming, security governance, dan lain sebagainya - pada peserta didik atau partisipan terkait.

Sementara itu secara giat berbagai praktisi maupun kelompok komunitas pun bertumbuhan di tanah air, dengan visi dan misi utama untuk mempromosikan dan meningkatkan kewaspadaan mengenai pentingnya keperdulian terhadap berinternet secara sehat dan aman. Penggiat komunitas ini berasal dari berbagai kalangan, seperti: praktisi teknologi informasi, lembaga swadaya masyarakat, organisasi politik, penggerak industri internet, pengusaha/vendor teknologi, dan lain sebagainya.

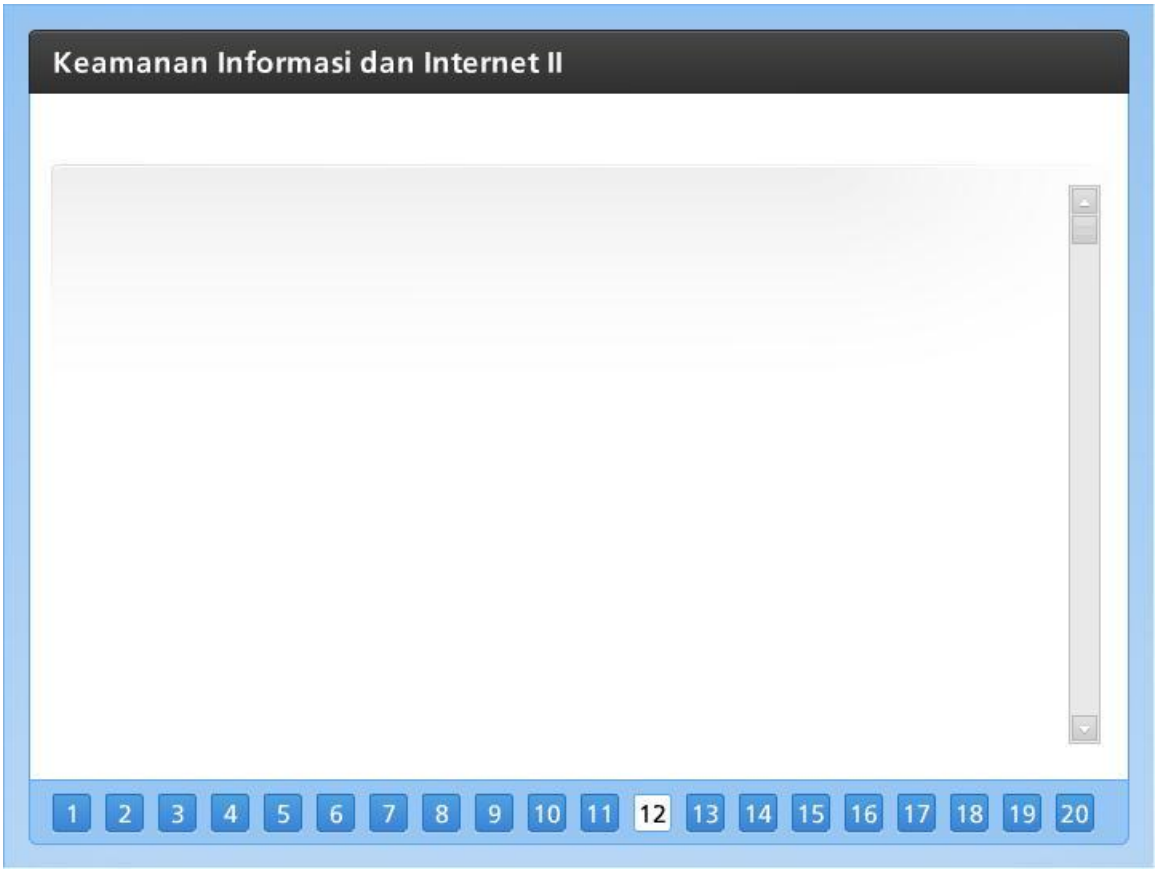
Terlepas dari berbagai bentuk, karakteristik, dan pendekatan aktivitas yang dilakukan, keseluruhan komponen organisasi tersebut di atas memiliki cita-cita dan obyektif yang sama, yaitu menyediakan lingkungan berinternet yang sehat dan aman.

Permasalahan yang Dihadapi

Terlepas dari begitu banyaknya usaha yang telah dilakukan secara kolektif tersebut, ada satu prinsip permasalahan keamanan informasi yang masih dihadapi dunia internet Indonesia. Kebanyakan aktivitas dan kegiatan yang dilakukan berbagai lembaga tersebut lebih fokus menggunakan pendekatan mengamankan infrastruktur jaringan internet dibandingkan dengan melakukan pengamanan terhadap data atau informasi yang mengalir pada infrastruktur jaringan tersebut. Kerawanan ini menimbulkan sejumlah potensi ancaman yang cukup serius sebagai berikut:

- kesulitan mengetahui tingkat integritas dan keaslian data yang diperoleh seandainya fasilitas pengaman jaringan gagal mendeteksi adanya modifikasi atau fabrikasi terhadap data yang dikirim (misalnya karena kualitas pengamanan yang buruk, anti virus yang tidak ter-update secara mutakhir, kecanggihan model penyerangan para kriminal, dan lain sebagainya);
- kemudahan pihak kriminal dalam mengerti data atau pesan yang dikirimkan setelah proses penyadapan, pengintaian, pengambilan, dan penduplikasian berhasil dilaksanakan terhadap informasi yang mengalir dalam sebuah jejaring internet yang aman maupun tidak aman (karena data atau pesan yang ada masih dalam bentuk asli tanpa dilakukan proses penyandian sama sekali);
- keleluasaan pihak kriminal dalam melakukan kegiatan kejahatannya seperti mencuri data dan informasi karena sebagian besar aset berharga tersebut masih tersimpan dalam bentuk plain file di dalam media penyimpanan semacam hard disk, CD ROM, flash disk, dan lain sebagainya;
- keterbukaan berbagai konten atau pesan komunikasi baik melalui media teknologi informasi maupun komunikasi seperti telepon genggam, Personal Digital Assistant, smart phone, communicator, blackberry, netbook, atau piranti gadget lainnya dalam bentuk SMS (Short Message Services), chatting, electronic mail, mailing list, newsgroup, dan lain-lain; serta
- kebiasaan individu atau masyarakat yang dengan mudahnya memberikan berbagai data dan informasi diri tanpa berpikir panjang terlebih dahulu karena kurang pahamnya mengenai potensi kejahatan yang dapat timbul di kemudian hari seperti yang ditunjukkan selama ini dalam berbagai konteksi seperti ketika berpartisipasi dalam

jejaring sosial internet, bertransaksi jual beli melalui situs e-commerce, beraktivitas menjadi anggota mailing list, bermain game berbasis jaringan, dan lain sebagainya.



Kriptologi dan Prinsip Keamanan Informasi

Dipandang dari sudut keamanan informasi berbasis digital atau data elektronik, sebagaimana layaknya uang bersisi dua (baca: two sides of a coin), ada dua aspek yang secara simultan harus diperhatikan secara sungguh-sungguh, yaitu keamanan fisik dan keamanan informasi. Yang dimaksud dengan keamanan fisik adalah terkait segala sesuatu yang berkaitan dengan usaha untuk mengamankan data dan informasi melalui mekanisme dan prosedur yang berhubungan dengan sumber daya yang dapat dilihat secara kasat mata (baca: fisik). Misalnya adalah bagaimana melakukan tindakan pengamanan terhadap fasilitas fisik seperti: kamera pengaman (baca: CCTV atau kamera surveillance), sensor jaringan, pintu pengaman pada data center, perimeter lokasi akses, penguncian port, alarm pengaman, kartu akses identifikasi, dan lain sebagainya.

Sementara untuk mengamankan informasi, berbagai cara pun kerap dipergunakan seperti: manajemen password, aplikasi anti virus, sistem deteksi terjadinya intrusi, pemutakhiran patches, dan lain sebagainya. Dari berbagai cara yang ada, ada satu mekanisme atau pendekatan

yang sangat efektif dan efisien untuk dapat diadopsi secara mudah, murah, dan masif - yaitu dengan memanfaatkan Kriptologi atau Ilmu Persandian - diambil dari bahasa Latin yang terdiri dari kata 'kriptos' (rahasia) dan 'logos' (ilmu). Dengan kata lain, kriptologi adalah ilmu atau seni yang mempelajari semua aspek tulisan rahasia.

Dalam tataran implementasinya, kriptologi dibagi menjadi dua, yaitu kriptografi dan kriptoanalisis. Kriptografi adalah cara, sistem, atau metode untuk mengkonstruksi pesan, berita, atau informasi sehingga menjadi tata tulisan yang berlainan dan tidak bermakna. Sementara kriptoanalisis adalah usaha untuk mendapatkan teks bermakna atau teks terang dari suatu teks dandi yang tidak diketahui sistem serta kunci-kuncinya. Dengan kata lain, kriptologi dapat dianggap sebagai sebuah ilmu atau seni untuk menjaga kerahasiaan berita - melalui penerapan sejumlah teknik-teknik matematika yang berhubungan dengan aspek keamanan data dan/atau informasi. Dari kedua hal ini, keberadaan kriptografi sangatlah dibutuhkan dalam konteks menjaga keamanan informasi di tanah air tercinta ini.

Paling tidak ada empat tujuan mendasar dari diberlakukannya kriptografi ini yang sangat erat kaitannya dengan aspek keamanan informasi, yaitu:

- Kerahasiaan Data - memastikan bahwa data atau informasi yang ada hanya dapat diakses oleh pihaki yang memiliiki otoritas atau wewenang, dengan cara menggunakan kunci rahasia yang menjadi miliknya untuk membuka dan/atau mengupas informasi yang telah disandi;
- Integritas Data - meyakinkan bahwa data atau informasi tertentu adalah utuh dan asli alias tidak terjadi aktivitas manipulasi data pihak-pihak yang tidak berhak, baik dalam bentuk pengubahan, penyisipan, penambahan, pengurangan, penghapusan, maupun pensubtitusian;
- Autentifikasi - memastikan bahwa data atau informasi yang dihasilkan memang benar-benar berasal dari pihak yang sebenarnya memiliki kewenangan untuk menciptakan atau berinteraksi dengan data/informasi tersebut; dan
- Non Repudiasi - meyakinkan bahwa benar-benar telah terjadi proses ataupun mekanisme tertentu yang terkait dengan keberadaan data/informasi dari pihak-pihak

yang berhubungan sehingga terhindar dari segala bentuk penyangkalan yang mungkin terjadi.

Teknik kriptografi atau lebih sederhananya dikenal sebagai proses penyandian ini dilakukan dengan menggunakan sejumlah algoritma matematik yang dapat memiliki kemampuan serta kekuatan untuk melakukan:

- konfusi atau pembingungan - merekonstruksi teks yang terang atau mudah dibaca menjadi suatu format yang membingungkan, dan tidak dapat dikembalikan ke bentuk aslinya tanpa menggunakan algoritma pembalik tertentu; dan
- difusi atau peleburan - melakukan mekanisme tertentu untuk menghilangkan satu atau sejumlah karakteristik dari sebuah teks yang terang atau mudah dibaca.

Sejumlah studi memperlihatkan bahwa di dunia nyata, kehandalan sebuah algoritma bukan terletak pada kerahasiaan algoritma itu sendiri, namun berada pada kuncinya. Secara prinsip algoritma yang dimaksud hanya melakukan dua proses transformasi, yaitu: enkripsi (proses transformasi mengubah teks terang atau plain text menjadi teks sandi atau cipher text) dan dekripsi (proses transformasi sebaliknya, yaitu merubah teks sandi menjadi teks terang). Adapun kunci yang dimaksud biasa dikenal sebagai istilah sederhana 'password', yang dalam implementasinya dapat berupa serangkaian campuran antara huruf, angka, dan simbol - hingga yang berbentuk biometrik seperti sidik jari, retina mata, karakter suara, suhu tubuh, dan berbagai kombinasi lainnya. Berbagai algoritma yang telah dikenal secara luas adalah Data Encryption Standard (DES), Blowfish, Twofish, MARS, IDEA, 3DES, dan AES (untuk tipe altoritma sandi kunci-simetris); atau Rivert-Shamir-Adelman (RSA), Knapsack, dan Diffie-Heillman (untuk tipe algoritma sandi kunci-asimetris).

Di samping itu, untuk semakin meningkatkan tingkat keamanan informasi, diperkenalkan pula sebuah fungsi hash Kriptologi seperti tipe MD4, MD5, SHA-0, SHA-1, SHA-256, dan SHA-512.

Budaya Penyandian dalam Masyarakat Indonesia

Kenyataan memperlihatkan - setelah dilakukan berbagai penelitian dan pengamatan - bahwa keperdulian masyarakat Indonesia tentang pentingnya menjaga kerahasiaan informasi masih sangatlah rendah. Ada sejumlah hal yang melatarbelakangi masih rendahnya keperdulian yang dimaksud. Pertama adalah masalah sosial budaya. Indonesia dikenal sebagai bangsa yang ramah

tamah, terutama dalam hal melayani orang-orang yang bertamu ke lokasi tempat tinggalnya - baik berasal dari dalam negeri maupun luar negeri. Disamping itu masyarakat Indonesia juga dikenal dengan kehidupan kolegialnya, dimana masing-masing individu memiliki hubungan kedekatan yang sangat kental - dengan fenomena utama saling bergantung, siap selalu memberikan bantuan, serta kerap merasa senasib sepenganggungan - dalam lingkungan komunitas berkeluarga, bertetangga, berorganisasi, berusaha, dan bermasyarakat. Demikian pula kecenderungan untuk memiliki banyak sahabat, tempat yang bersangkutan mencurahkan segenap permasalahan, isi hati, pendapat, ajakan, maupun ketidaksetujuan menunjukkan adanya budaya 'trust' atau kepercayaan yang tinggi pada orang lain. Hal inilah yang menyebabkan timbulnya kebiasaan untuk senang menyebarkan berita, membagi informasi, menyerahkan data, menitipkan pesan, serta perilaku terbuka lainnya tanpa adanya upaya filterisasi maupun penyandian - karena hal tersebut dianggap menyalahi prinsip keterbukaan dan keterpercayaan yang telah dibangun selama ini.

Kedua adalah masalah pendidikan. Tidak banyak orang yang mengerti dan memahami betapa pentingnya nilai dari sebuah aset yang bernama data atau informasi dewasa ini. Hanya segelintir masyarakat yang pernah membaca, mendengar, melihat, membahas, dan mensinyalir adanya peristiwa buruk dalam kehidupan akibat dari berbagai permasalahan terkait dengan keterbukaan data dan informasi. Banyak yang lupa atau kurang paham, bahwa fenomena dis-informasi dan mis-informasi misalnya dapat mengakibatkan terjadinya kerusuhan, kekacauan, bahkan ke-arnakisan di kalangan masyarakat akar rumput. Prinsip 'perception is reality' merupakan kata kunci yang kerap dipergunakan oleh pihak yang tidak bertanggung jawab dalam mencoba mempengaruhi dan membentuk opini serta persepsi masyarakat melalui pengrusakan atau penyesatan informasi - dengan cara menyadap, merubah, merusak, mengganti, memodifikasi, mengkonstruksi ulang, bahkan menghilangkan hal-hal yang seharusnya sangat bernilai dan diperlukan oleh pihak-pihak tertentu dan masyarakat. Masalah pendidikan ini wajar adanya, karena memang selain Indonesia masih merupakan sebuah negara berkembang yang sedang berjuang keluar dari kemiskinan dan kebodohan, teknologi informasi dan komunikasi tumbuh berkembang sedemikian pesatnya, yang membutuhkan kemauan dan kemampuan dari masyarakat moderen untuk dapat mengerti dampak negatif yang mungkin ditimbulkan dan mencari cara mengatasinya. Begitu banyak masyarakat moderen yang terbuai dengan berbagai kemajuan dan perubahan dinamika dunia global yang terjadi, tanpa sempat memikirkan kemungkinan terjadinya dampak negatif di kemudian hari.

Ketiga adalah masalah teknis. Ada dua aspek yang berkaitan dengan hal ini. Pertama adalah kemampuan, dalam arti kata telah cukup banyak masyarakat golongan menengah yang tahu akan pentingnya menjaga kerahasiaan data melalui mekanisme kriptografi. Namun pada saat bersamaan, yang bersangkutan tidak tahu bagaimana cara melakukannya. Misalnya adalah pemakai setia email dan SMS, yang tidak tahu bagaimana melakukan aktivitas enkripsi maupun dekripsi walaupun komputer atau piranti telepon genggamnya menyediakan hal tersebut. Demikian pula halnya dengan pemakai blackberry, mailing list, Facebook, Twitters, Friendsters, dan lain sebagainya. Kedua adalah kemauan untuk melakukan hal tersebut, karena selain dipandang rumit, proses enkripsi dan dekripsi memerlukan aktivitas tambahan yang lumayan memakan waktu dan usaha. Sangat sulit dirasakan untuk menanamkan kesadaran, keperdulian, dan motivasi individu agar dengan kesadarannya menggunakan ilmu Kriptologi untuk mengamankan transaksi, komunikasi, dan interaksi mereka. Konsep 'tahu, mau, dan bisa' nampaknya harus senantiasa ditanamkan kepada setiap individu yang tidak ingin menjadi korban kejahatan.

Keempat adalah masalah hukum. Walaupun hingga kini telah ada seperangkat peraturan dan perundang-undangan yang secara langsung maupun tidak langsung mengatur hukuman bagi siapa saja yang melakukan kejahatan keamanan informasi seperti UU Telekomunikasi dan UU Informasi dan Transaksi Elektronik misalnya, namun belum ada cukup aturan yang mengharuskan pihak-pihak tertentu untuk menjalankan aktivitas penyandian dalam berbagai aktivitas kegiatannya. Contohnya adalah aturan yang mengikat dan tegas terhadap perlunya dilakukan proses penyandian dalam berbagai tingkatan interaksi pada setiap institusi atau obyek vital kenegaraan, seperti: instalasi militer, pusat pertambangan, bandara udara, simpul transaksi keuangan, pembangkit listrik, dan lain sebagainya. Tidak adanya keharusan atau peraturan yang mengatur sering diartikan dengan tidak adanya urgensi untuk melakukan hal yang dimaksud.

Selain empat masalah besar yang mendominasi tersebut, masih banyak terdapat isu-isu lainnya yang kerap menghambat terbentuknya budaya kriptografi atau penyandian di tengah-tengah masyarakat Indonesia, seperti misalnya: masalah kebiasaan, masalah insentif, masalah kepercayaan, masalah kepasrahan, masalah perilaku, masalah kemalasan, masalah keengganan dan lain sebagainya. Secara tidak langsung hal ini memperlihatkan bahwa masyarakat Indonesia masih merupakan komunitas berbudaya 'risk taker' atau berani menghadapi resiko apa pun yang mungkin terjadi di masa mendatang akibat kecerobohan dalam mengamankan informasi.

Dampak dan Resiko Perang di Dunia Maya

Banyak orang tidak tahu bahwa sebenarnya saat ini 'perang besar' di dunia maya tengah terjadi akibat globalisasi dan perkembangan teknologi informasi dan komunikasi. Selama tahun 2009 contohnya, ID-SIRTII mencatat bahwa setiap harinya, paling tidak terdapat rata-rata satu setengah juta percobaan serangan yang diarahkan untuk melumpuhkan internet Indonesia dengan berbagai modus kejahatan yang dilakukan baik dari luar negeri maupun dari dalam negeri sendiri. Jenis kajahatan yang dilakukan pun sangatlah beragam, yang secara kategori dapat dibagi menjadi empat jenis:

- Intersepsi - yang merupakan usaha untuk melakukan penyadapan terhadap sejumlah pesan, berita, data, atau informasi yang mengalir di dalam pipa transmisi internet Indonesia oleh pihak yang tidak berwenang dengan jenis serangan semacam sniffing dan eavesdropping;
- Interupsi - yang merupakan usaha untuk mengganggu hubungan komunikasi antar sejumlah pihak melalui berbagai cara seperti serangan bertipe DOS (Denial Of Services), DDOS (Distributed Denial Of Services), botnet, package flooding, dan lain sebagainya;
- Modifikasi - yang merupakan usaha melakukan perubahan terhadap pesan, berita, data, atau informasi yang mengalir pada pipa transmisi untuk memfitnah, mengelabui, membohongi, atau menyebarkan hal-hal yang tidak baik melalui mekanisme serangan semacam web defacement, SQL injection, cross scripting, dan beragam variasi lainnya; serta
- Fabrikasi - yang merupakan usaha untuk mengelabui pihak lain melalui beragam proses penyamaran terselubung dengan seolah-olah menjadi pihak yang memiliki wewenang atau hak akses yang sah, misalnya dengan menggunakan pendekatan serangan seperti phishing atau spoofing.

Seperti halnya perang di dunia fisik, perang di dunia maya telah banyak menelan korban dengan angka kerugian yang besarnya berkali-kali lipat dibandingkan dengan perang konvensional. Namun anehnya, karena kebanyakan sifatnya yang intangible, banyak masyarakat Indonesia yang tidak merasa telah kehilangan sesuatu atau merasa telah mengalami kerugian yang berarti. Cobalah lihat sejumlah peristiwa yang mungkin akan atau telah terjadi selama ini, seperti:

- Berapa banyak aset dokumen berharga berisi resep, formula, rahasia dagang, karya cipta, temuan, rancangan teknis, maupun paten produk yang telah jatuh ke tangan pihak asing karena dicuri melalui internet atau mekanisme lain di dunia maya;
- Seberapa banyak informasi rahasia seperti password, nomor kartu kredit, nama ibu kandung, nomor rekening, data kesehatan, profil pribadi, dan lain-lain yang telah bocor dan dikoleksi oleh para kriminal untuk selanjutnya diperjual-belikan di pasar hitam 'underground economy';
- Berapa banyak percakapan rahasia, dokumen penting, interaksi tertutup, maupun kegiatan intelijen yang berhasil diketahui dengan mudah oleh pihak yang tidak berwenang karena kemahiran mereka dalam menembus pertahanan jaringan pengaman sistem tempat disimpannya data penting atau terjadinya interaksi yang bersifat rahasia; dan
- Seberapa banyak aset tangible yang akhirnya harus direlakan untuk menjadi milik asing atau negara lain akibat sering kalahnya Indonesia dalam menghadapi perang citra di dunia maya karena banyaknya pihak-pihak yang melakukan aktivitas semacam kontra intelijen, mata-mata, negative marketing, public relations, dan black campaign.

Kalau hal ini terus dibiarkan terjadi, dimana aset yang paling berharga di era globalisasi ini - yaitu informasi dan pengetahuan - dibiarkan menjadi sebuah entitas yang 'telanjang' dan 'terang benderang' karena tidak dibalut dengan keamanan informasi melalui teknik persandian - maka perlahan namun pasti, tidak mustahil Indonesia akan menjadi layaknya kapal raksasa Titanic yang perlahan tenggelam.

Gerakan Nasional Penerapan Kriptografi

Mempelajari semua hal di atas, tidak ada jalan lain bagi bangsa Indonesia untuk dapat tetap bertahan di tengah persaingan global yang serba terbuka ini untuk segera melindungi dirinya dari berbagai serangan yang terjadi setiap hari di dunia maya. Harus ada sebuah usaha yang sistematik, berskala nasional dan bersifat masif, untuk menyadarkan seluruh masyarakat akan pentingnya menjaga keamanan informasi melalui penerapan kriptografi. Lembaga Sandi Negara sebagai sebuah institusi yang memiliki kewenangan, kekuatan, kompetensi, keahlian, dan kepiawaian di bidang kriptologi haruslah dapat menjadi lokomotif terdepan dalam memimpin gerakan ini. Prinsip dalam dunia keamanan informasi yang mengatakan bahwa 'your security is my security' memberikan arti bahwa gerakan sosialisasi keperdulian dan penyadaran akan pentingnya menerapkan kriptografi tersebut harus menyentuh seluruh lapisan hidup

masyarakat, tanpa mengenal usia, latar belakang, status ekonomi, faksi politik, dan perbedaan-perbedaan lainnya. Gerakan tersebut harus mengakar dalam setiap kehidupan masyarakat moderen, dimana kelak akan menjadi sebuah budaya yang menyatu dengan kebiasaan, perilaku, serta tindakan individu-individu di tanah air.

Agar efektif, maka gerakan yang dimaksud harus dilakukan secara simultan dengan menggunakan pendekatan top-down dan bottom-up sebagai berikut:

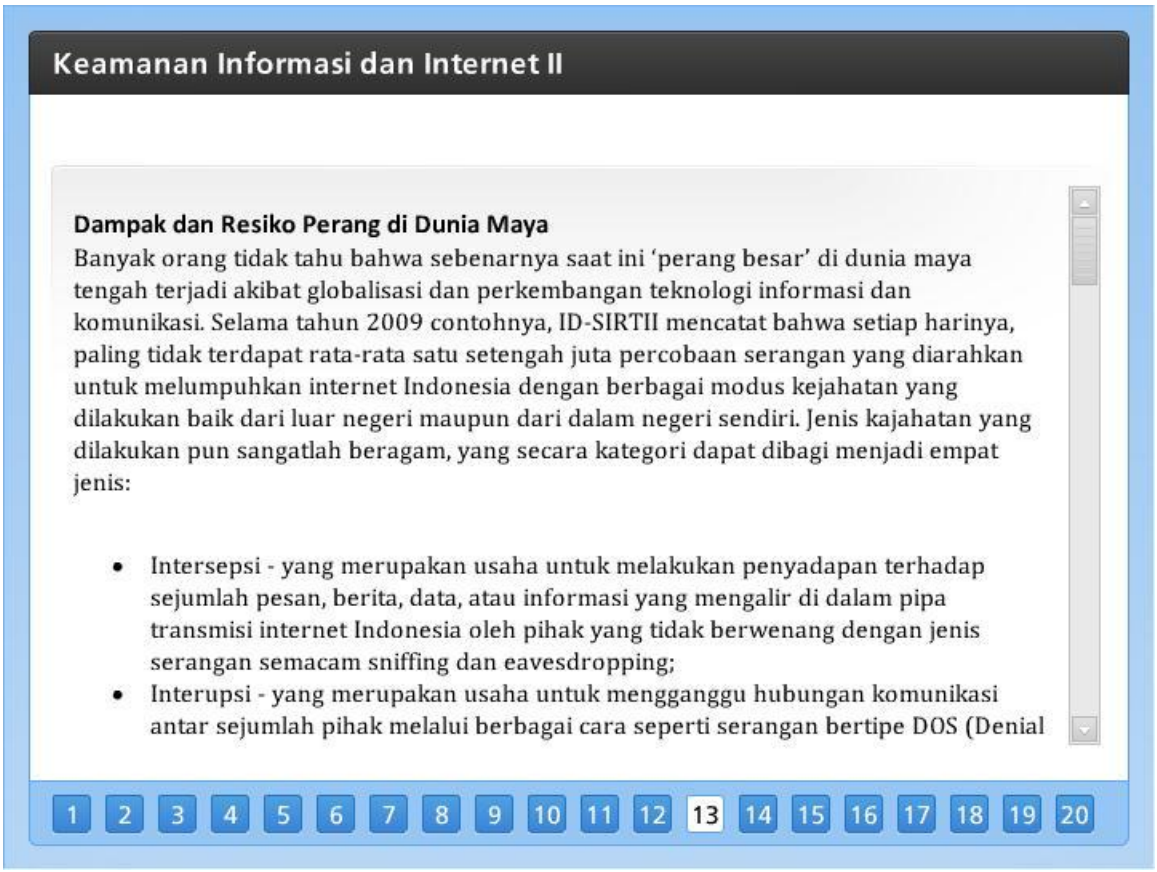
- Pendekatan Top Down - berupa usaha pemerintah dan negara dalam mensosialisasikan secara tiada henti, konsisten, persistence, dan berkesinambungan terhadap pentingnya setiap individu dan komponen kehidupan masyarakat dalam melakukan pengamanan terhadap aset data maupun informasi yang dimiikinya - misalnya adalah dengan melakukan teknik kriptografi. Khusus untuk institusi atau organisasi yang bertanggung jawab terhadap kelangsungan operasional obyek-obyek vital negara - yang secara langsung menyangkut hajat hidup orang banyak - perlu diberlakukan peraturan yang ketat berisi keharusan dalam menerapkan kriptografi dalam aktivitas kegiatannya sehari-hari. Mekanisme 'reward and punishment' perlu secara tegas dikembangkan dan diterapkan dalam konteks ini; yang tentu saja berjalan dengan proses penegakan hukum yang adil dan berwibawa.
- Pendekatan Bottom Up - merupakan akumulasi dari kegiatan kolektif komunitas basis akar rumput, akademisi, industri swasta, maupun organisasi non profit lainnya dalam membangun kesadaran akan pentingnya menjaga kemanan informasi sesuai dengan konteks dan peranannya masing-masing. Melalui program edukatif semacam seminar, lokakarya, workshop, pelatihan, diskusi, dan tanya jawab hingga yang bersifat komersil seperti proyek pengembangan sistem pengamanan, konsultasi standar keamanan informasi, jual beli alat-alat produk keamanan, riset dan pengembangan algoritma kriptografi, pengalihdayaan (baca: outsourcing) jasa keamanan informasi, dan lain sebagainya - masyarakat berperan secara aktif membentuk lingkungan yang kondusif dalam mengembangkan budaya dan ekosistem keamanan informasi.

Dengan bertemunya kedua sisi 'demand' dan 'supply' di atas - yaitu antar kebutuhan yang diciptakan melalui pendekatan 'top down' dan ketersediaan yang dipicu melalui penekatan 'bottom up' - maka nischaya akan terbentuk dan terbangun ekosistem keamanan informasi dan internet yang tangguh di tanah air tercinta ini.

Penutup

Pada akhirnya, hakekat dari keamanan informasi itu melekat pada diri masing-masing individu. Topologi atau postur internet yang menghubungkan beribu-ribu bahkan berjuta-juta titik koneksi secara eksplisit memperlihatkan bahwa 'the stength of a chain depends on the weakest link' atau dalam bahasa Indonesianya 'kekuatan sebuah rantai terletak pada mata sambungan yang paling lemah'. Artinya adalaah bahwa tidak ada gunanya jika hanya sebagian kecil masyarakat saja yang paham dan perduli akan keamanan informasi, sementara masih banyak pihak lain yang tidak mau tahu mengenai pentingnya usaha bersama untuk mengamankan diri.

Perlu diingat, bahwa tidak ada negara di dunia ini yang meluangkan waktunya atau mengalokasikan sumber dayanya untuk melindungi keamanan informasi dari negara lain. Keamanan ekosistem internet Indonesia sepenuhnya terletak pada masyarakat Indonesia itu sendiri - yang pada akhirnya ditentukan oleh 'budaya aman' dari setiap insan atau individu manusia nusantara yang tersebar dari Sabang sampai Merauke, tanpa kecuali.



Dampak dan Resiko Perang di Dunia Maya

Banyak orang tidak tahu bahwa sebenarnya saat ini 'perang besar' di dunia maya tengah terjadi akibat globalisasi dan perkembangan teknologi informasi dan komunikasi. Selama tahun 2009 contohnya, ID-SIRTII mencatat bahwa setiap harinya, paling tidak terdapat rata-rata satu setengah juta percobaan serangan yang diarahkan untuk melumpuhkan internet Indonesia dengan berbagai modus kejahatan yang dilakukan baik dari luar negeri maupun dari dalam negeri sendiri. Jenis kajahatan yang dilakukan pun sangatlah beragam, yang secara kategori dapat dibagi menjadi empat jenis:

- Intersepsi - yang merupakan usaha untuk melakukan penyadapan terhadap sejumlah pesan, berita, data, atau informasi yang mengalir di dalam pipa transmisi internet Indonesia oleh pihak yang tidak berwenang dengan jenis serangan semacam sniffing dan eavesdropping;
- Interupsi - yang merupakan usaha untuk mengganggu hubungan komunikasi antar sejumlah pihak melalui berbagai cara seperti serangan bertipe DOS (Denial Of Services), DDOS (Distributed Denial Of Services), botnet, package flooding, dan lain sebagainya;
- Modifikasi - yang merupakan usaha melakukan perubahan terhadap pesan, berita, data, atau informasi yang mengalir pada pipa transmisi untuk memfitnah, mengelabui, membohongi, atau menyebarkan hal-hal yang tidak baik melalui mekanisme serangan semacam web defacement, SQL injection, cross scripting, dan beragam variasi lainnya; serta
- Fabrikasi - yang merupakan usaha untuk mengelabui pihak lain melalui beragam proses penyamaran terselubung dengan seolah-olah menjadi pihak yang memiliki wewenang atau hak akses yang sah, misalnya dengan menggunakan pendekatan serangan seperti phishing atau spoofing.

Seperti halnya perang di dunia fisik, perang di dunia maya telah banyak menelan korban dengan angka kerugian yang besarnya berkali-kali lipat dibandingkan dengan perang konvensional. Namun anehnya, karena kebanyakan sifatnya yang intangible, banyak masyarakat Indonesia yang tidak merasa telah kehilangan sesuatu atau merasa telah mengalami kerugian yang berarti. Cobalah lihat sejumlah peristiwa yang mungkin akan atau telah terjadi selama ini, seperti:

- Berapa banyak aset dokumen berharga berisi resep, formula, rahasia dagang, karya cipta, temuan, rancangan teknis, maupun paten produk yang telah jatuh ke tangan pihak asing karena dicuri melalui internet atau mekanisme lain di dunia maya;
- Seberapa banyak informasi rahasia seperti password, nomor kartu kredit, nama ibu kandung, nomor rekening, data kesehatan, profil pribadi, dan lain-lain yang telah bocor dan dikoleksi oleh para kriminal untuk selanjutnya diperjual-belikan di pasar hitam 'underground economy';
- Berapa banyak percakapan rahasia, dokumen penting, interaksi tertutup, maupun kegiatan intelijen yang berhasil diketahui dengan mudah oleh pihak yang tidak berwenang karena kemahiran mereka dalam menembus pertahanan jaringan pengaman sistem tempat disimpannya data penting atau terjadinya interaksi yang bersifat rahasia; dan
- Seberapa banyak aset tangible yang akhirnya harus direlakan untuk menjadi milik asing atau negara lain akibat sering kalahnya Indonesia dalam menghadapi perang citra di dunia maya karena banyaknya pihak-pihak yang melakukan aktivitas semacam kontra intelijen, mata-mata, negative marketing, public relations, dan black campaign.

Kalau hal ini terus dibiarkan terjadi, dimana aset yang paling berharga di era globalisasi ini - yaitu informasi dan pengetahuan - dibiarkan menjadi sebuah entitas yang 'telanjang' dan 'terang benderang' karena tidak dibalut dengan keamanan informasi melalui teknik persandian - maka perlahan namun pasti, tidak mustahil Indonesia akan menjadi layaknya kapal raksasa Titanic yang perlahan tenggelam.

Gerakan Nasional Penerapan Kriptografi

Mempelajari semua hal di atas, tidak ada jalan lain bagi bangsa Indonesia untuk dapat tetap bertahan di tengah persaingan global yang serba terbuka ini untuk segera melindungi dirinya dari berbagai serangan yang terjadi setiap hari di dunia maya. Harus ada sebuah usaha yang sistematik, berskala nasional dan bersifat masif, untuk menyadarkan seluruh masyarakat akan pentingnya menjaga keamanan informasi melalui penerapan kriptografi. Lembaga Sandi Negara sebagai sebuah institusi yang memiliki kewenangan, kekuatan, kompetensi, keahlian, dan kepiawaian di bidang kriptologi haruslah dapat menjadi lokomotif terdepan dalam memimpin gerakan ini. Prinsip dalam dunia keamanan informasi yang mengatakan bahwa 'your security is my security' memberikan arti bahwa gerakan sosialisasi keperdulian dan penyadaran akan pentingnya menerapkan kriptografi tersebut harus menyentuh seluruh lapisan hidup

masyarakat, tanpa mengenal usia, latar belakang, status ekonomi, faksi politik, dan perbedaan-perbedaan lainnya. Gerakan tersebut harus mengakar dalam setiap kehidupan masyarakat moderen, dimana kelak akan menjadi sebuah budaya yang menyatu dengan kebiasaan, perilaku, serta tindakan individu-individu di tanah air.

Agar efektif, maka gerakan yang dimaksud harus dilakukan secara simultan dengan menggunakan pendekatan top-down dan bottom-up sebagai berikut:

- Pendekatan Top Down - berupa usaha pemerintah dan negara dalam mensosialisasikan secara tiada henti, konsisten, persistence, dan berkesinambungan terhadap pentingnya setiap individu dan komponen kehidupan masyarakat dalam melakukan pengamanan terhadap aset data maupun informasi yang dimiikinya - misalnya adalah dengan melakukan teknik kriptografi. Khusus untuk institusi atau organisasi yang bertanggung jawab terhadap kelangsungan operasional obyek-obyek vital negara - yang secara langsung menyangkut hajat hidup orang banyak - perlu diberlakukan peraturan yang ketat berisi keharusan dalam menerapkan kriptografi dalam aktivitas kegiatannya sehari-hari. Mekanisme 'reward and punishment' perlu secara tegas dikembangkan dan diterapkan dalam konteks ini; yang tentu saja berjalan dengan proses penegakan hukum yang adil dan berwibawa.
- Pendekatan Bottom Up - merupakan akumulasi dari kegiatan kolektif komunitas basis akar rumput, akademisi, industri swasta, maupun organisasi non profit lainnya dalam membangun kesadaran akan pentingnya menjaga kemanan informasi sesuai dengan konteks dan peranannya masing-masing. Melalui program edukatif semacam seminar, lokakarya, workshop, pelatihan, diskusi, dan tanya jawab hingga yang bersifat komersil seperti proyek pengembangan sistem pengamanan, konsultasi standar keamanan informasi, jual beli alat-alat produk keamanan, riset dan pengembangan algoritma kriptografi, pengalihdayaan (baca: outsourcing) jasa keamanan informasi, dan lain sebagainya - masyarakat berperan secara aktif membentuk lingkungan yang kondusif dalam mengembangkan budaya dan ekosistem keamanan informasi.

Dengan bertemunya kedua sisi 'demand' dan 'supply' di atas - yaitu antar kebutuhan yang diciptakan melalui pendekatan 'top down' dan ketersediaan yang dipicu melalui penekatan 'bottom up' - maka nischaya akan terbentuk dan terbangun ekosistem keamanan informasi dan internet yang tangguh di tanah air tercinta ini.

Penutup

Pada akhirnya, hakekat dari keamanan informasi itu melekat pada diri masing-masing individu. Topologi atau postur internet yang menghubungkan beribu-ribu bahkan berjuta-juta titik koneksi secara eksplisit memperlihatkan bahwa 'the stength of a chain depends on the weakest link' atau dalam bahasa Indonesianya 'kekuatan sebuah rantai terletak pada mata sambungan yang paling lemah'. Artinya adalaah bahwa tidak ada gunanya jika hanya sebagian kecil masyarakat saja yang paham dan perduli akan keamanan informasi, sementara masih banyak pihak lain yang tidak mau tahu mengenai pentingnya usaha bersama untuk mengamankan diri.

Perlu diingat, bahwa tidak ada negara di dunia ini yang meluangkan waktunya atau mengalokasikan sumber dayanya untuk melindungi keamanan informasi dari negara lain. Keamanan ekosistem internet Indonesia sepenuhnya terletak pada masyarakat Indonesia itu sendiri - yang pada akhirnya ditentukan oleh 'budaya aman' dari setiap insan atau individu manusia nusantara yang tersebar dari Sabang sampai Merauke, tanpa kecuali.