

Siapa Perlu Peduli Ancaman Cybercrime?

Oleh: **Mas Wigrantoro Roes Setiyadi***)

Kelompok Kerja e-Security, suatu unit aktivitas di dalam wadah Organisasi Kerjasama Ekonomi Asia Pacific (APEC) kembali menggelar Konferensi Cybercrime dengan mengambil thema “Membangun Kapasitas Penegak Hukum dan Legislasi Untuk Memerangi Cybercrime”. Setelah dua kali peristiwa serupa diselenggarakan di Bangkok (2003) dan Hanoi (2004), konferensi kali ini mengambil tempat di Seoul, Korea. Agenda utama konferensi membahas persoalan yang dihadapi dalam proses legislasi dan peningkatan kapasitas penegak hukum di bidang cyber. Indonesia diwakili oleh lima orang peserta, masing – masing dua orang dari Bank Indonesia, satu orang dari Departemen Kominfo (Staf Ahli Menteri), satu orang dari Fakultas Hukum Universitas Indonesia, dan penulis mewakili sektor swasta.

Kejahatan yang dilakukan melalui atau terjadi di lingkungan Internet (Cybercrime) sudah lama menjadi perhatian serius berbagai kalangan di seluruh dunia. Pada masa Internet baru diperkenalkan untuk dipakai kalangan sipil, frekuensi kejahatan masih sedikit begitupun modusnya masih sederhana, sehingga dampak negatif yang dihasilkan masih belum dianggap sebagai ancaman serius bagi masyarakat dunia. Seiring perkembangan Internet yang semakin canggih dan mengglobal, demikian pula insiden cybercrime mengalami perkembangan yang sangat pesat. Angka kerugian melewati setengah milyar US\$, demikian pula sebaran korbannyapun makin meluas, di wilayah Asia Pasifik dan Eropa, dilaporkan tidak ada negara yang belum pernah menjadi korban cybercrime.

Dilihat dari jenis serangan, selain cara konvensional yang masih dilakukan seperti pembuatan dan pengiriman virus, akses ilegal dengan memalsukan identitas, perusakan situs Internet (*hacking* dan *cracking*), pengiriman spam, dan lain sebagainya belakangan ini muncul modus kejahatan baru yang diberi nama *Phishing* dan *Botnet*. Dilaporkan, *phishing* telah merugikan banyak lembaga bisnis seperti bank, penerbit kartu kredit, dan

penyelenggara e-commerce seperti e-Bay dan PayPal. Cara kerja *phishing* adalah dengan mengirim email palsu atau *spam* yang seolah dikirim oleh insitusi bisnis terkenal dengan maksud merayu atau menawarkan layanan tertentu, agar penerima email memberikan *username, password, account-ID* yang ada pada kartu kredit atau ATM yang dimilikinya. Penerima email tidak menyadari bahwa mereka telah digiring masuk ke suatu situs palsu yang dimaksudkan untuk mengumpulkan data nasabah atau pemegang kartu kredit, kartu ATM, dan lainnya. Data tersebut kemudian digunakan oleh pelaku kejahatan untuk membuat transaksi, mengambil/transfer uang atau membeli sesuatu dari situs yang sah.

Botnet belakangan menjadi perhatian karena penyerang dapat mengendalikan personal komputer secara jarak jauh tanpa disadari oleh pemiliknya untuk menyerang komputer lain, mengirim *spam*, menghentikan layanan (DDOS), mengintai aktivitas seseorang, menyebarkan virus, mencuri informasi sensitif (*key-logging*), dan lain sebagainya. Dalam kata lain, suatu komputer yang telah dijadikan botnet seolah menjadi “budak” atau perantara (*messenger*) yang dapat melakukan apa saja tanpa diketahui pemiliknya.

Munculnya berbagai jenis kejahatan cyber di atas, dan makin menyebarnya penggunaan Internet untuk mendukung aktivitas bisnis dan pemerintahan mendorong perlunya peningkatan upaya pencegahan dan penindakan terhadap pelaku kejahatan cyber. Peningkatan upaya pencegahan dilakukan dengan sosialisasi pemanfaatan komputer secara lebih aman, bagi diri sendiri maupun orang lain. Aktivitas edukasi masyarakat ini sebaiknya dilakukan di sekolah – sekolah, perguruan tinggi, lembaga kursus yang menggunakan komputer, instansi pemerintah dan swasta, sarana akses informasi publik, maupun melalui berbagai kegiatan sosial masyarakat lainnya yang berkaitan dengan akses dan penyebaran informasi melalui Internet.

Berkaitan dengan sosialisasi pemanfaatan komputer secara lebih aman, hal penting kedua yang perlu menjadi perhatian bagi semua pihak adalah bahwa ancaman cyber crime yang berujung pada kerugian moril dan material dan dapat menimpa siapa saja. Jika dilihat dari statistik pemilik dan pengguna komputer dan Internet di Indonesia memang angkanya masih relatif kecil dibandingkan populasi penduduk, namun demikian potensi kerugian

yang ditimbulkannya tidak berbanding lurus dengan jumlah pengguna, atau dengan kata lain potensi kerugian tidak dapat diperkirakan nilainya maupun jumlah korbannya. Sebagai contoh, kerugian yang menimpa lembaga sebuah lembaga perbankan di suatu anggota APEC akibat *phising* dilaporkan hampir membuat bank tersebut harus menutup layanannya karena selain bank tersebut merugi, juga harus menanggung tuntutan dari nasabah yang dirugikan karena sistem keamanannya lemah.

Industri perbankan merupakan salah satu sasaran kejahatan cybercrime yang memiliki potensi kerugian besar sekali, apalagi dengan mulai berlakunya layanan perbankan secara elektronik dalam bentuk *e-banking* dan *electronic fund transfer*. Sektor lembaga keuangan lain yang rentan terhadap serangan cybercrime termasuk jasa asuransi, pembiayaan (*leasing*), bursa saham, bursa komoditi, dan perdagangan valas. Namun sayangnya perhatian dan dukungan dari kalangan industri perbankan maupun lembaga keuangan lainnya terhadap penanggulangan masalah cybercrime di Indonesia masih tergolong minimal. Masih rendahnya kepedulian terhadap ancaman cybercrime di Indonesia juga ditunjukkan oleh pelaku ekonomi di sektor – sektor lain, seperti perdagangan, perhubungan, dan lembaga penyedia layanan publik. Sebagai mana diketahui, perkembangan penggunaan komputer khususnya Internet di kalangan perusahaan swasta sebagai sarana operasional dan manajerial sudah cukup maju. Ada kecenderungan, semakin maju (*advance*) dalam memanfaatkan komputer dan Internet , kinerja perusahaan akan semakin tergantung kepada komputer dan Internet yang dikelolanya dalam suatu sistem informasi. Persoalannya, jika sistem informasi berbasis komputer/Internet tersebut mengalami gangguan akibat kejahatan, dapat dipastikan perusahaan akan mengalami guncangan yang luar biasa besarnya. Banyak eksekutif petinggi perusahaan yang belum menyadari hal ini, mereka masih beranggapan bahwa keberadaan komputer dan sistem informasi masih belum menjadi bagian integral dari strategi bisnis, sehingga akibatnya mereka merasa tidak perlu peduli terhadap ancaman kejahatan cyber yang sewaktu – waktu dapat menyerang.

Keengganan mendukung upaya perang terhadap kejahatan cyber dengan memperkuat kapasitas aparat penegak hukum dan membentuk undang – undang anti kejahatan cyber

juga ditunjukkan oleh birokrat dan para politisi di Parlemen. Indikasi keengganan Parlemen ini setidaknya terlihat dari komentar beberapa anggota Dewan tentang masih belum perlunya Indonesia memiliki cyberlaw karena pengguna komputer masih sedikit, didominasi orang kaya, dan terpusat di perkotaan. Ada juga anggota Dewan yang masih mempertanyakan perusahaan atau pihak mana yang menjadi sponsor dan berkepentingan terhadap dibentuknya cyberlaw. Kondisi di kalangan birokrasi tidak jauh berbeda dengan Parlemen, persoalan ancaman cyber dilihat sebagai persoalan sektoral, urusan Kementerian Kominfo (sekarang menjadi Departemen Komunikasi dan Informatika). Padahal, perlu diketahui bahwa seluruh instansi pemerintah dari pusat sampai daerah yang menggunakan komputer memiliki potensi menjadi korban kejahatan cyber.

Uraian di atas berusaha menjelaskan, siapa saja - tanpa kecuali - yang menggunakan komputer baik untuk dipakai secara *stand alone*, terhubung ke suatu jaringan lokal, atau terhubung ke jaringan global (Internet) memiliki peluang untuk menjadi korban kejahatan cyber. Berbeda dengan kejahatan konvensional yang dampaknya relatif mudah dilokalisasi, maksimum nilai kerugiannya sebesar nilai yang melekat pada sasaran kejahatan, pada kejahatan cyber pelaku dan korban tidak harus berada pada dimensi ruang dan waktu yang sama, sehingga lebih sulit untuk dilokalisir pelakunya, dan nilai kerugian yang ditimbulkannya tidak terbatas pada nilai material yang melekat pada sasaran, artinya nilai kerugian seringkali jauh lebih besar dan bahkan sering tak ternilai harganya. Sebagai contoh, suatu kejahatan cyber menyerang sistem komputer milik suatu bank, yang menjadi sasaran langsung (diserang melalui Internet) adalah satu unit komputer yang berfungsi sebagai *data base server* dengan nilai fisik – misalnya – Rp. 100 juta, di dalam *server* ini tersimpan *data base* nasabah, transaksi perbankan dan data penting lainnya yang nilainya tak terhingga besarnya, *data base server* ini terhubung ke sejumlah *workstation* dan *server* aplikasi yang di dalamnya terdapat aplikasi perbankan dengan total nilai – misalnya – Rp. 50 milyar rupiah. Kejahatan cyber tidak perlu merusak fisik seluruh *workstation* dan kedua *server* tersebut, namun kerugian yang menimpa bank tersebut bisa mencapai setidaknya Rp. 50 milyar karena perusakan aplikasi piranti lunak, atau maksimum tak terhingga besarnya karena perusakan *record* di dalam *database*.

Pertanyaannya, selain pemahaman terhadap bahaya cybercrime oleh seluruh elemen masyarakat, hal mendesak apa yang perlu dikerjakan dalam upaya memerang kejahatan cyber? Dan siapa pula yang harus melaksanakannya? Jawabannya hanya dua. Pertama, Indonesia harus segera memiliki undang – undang yang mengatur tentang pemanfaatan teknologi informasi (cyberlaw), termasuk dalam kelompok ini adalah undang – undang tindak pidana teknologi informasi (cyber crime law), Dan kedua, Pemerintah Republik Indonesia harus segera memberi perhatian besar kepada upaya peningkatan kapasitas penegak hukum (polisi, jaksa, dan hakim) untuk memerangi kejahatan cyber.

*) *Direktur*, Institute for Technology and Economic Policy Studies <<INSTEPS>>
Ketua, Masyarakat Telematika Indonesia [MASTEL]