MODUS, PENYEBAB DAN STRATEGI PENANGGULANGAN CYBERCRIME

Dahlia Br Ginting

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda 96 Bandung 40132

e-mail: dahliaginting@yahoo.co.id

ABSTRAK

Perkembangan internet yang semakin pesat, selain membawa dampak positif bagi umat manusia, di sisi lain juga mengundang tangan-tangan criminal untuk bereaksi, baik untuk mencari keuntungan materi maupun sekedar melampiaskan keisengan. Hal ini memunculkan fenomena khas yang sering disebut *cybercrime* atau kejahatan di dunia maya. *Cybercrime* sering dilakukan secara transnasional, melintasi batas antar negara sehingga sulit dipastikan yuridiksi hukum negara mana yang diberlakukan. Karakteristik internet dimana orang dapat berlalu lalang tanpa identitas (*anonymous*), hal ini sangat memungkinkan terjadinya berbagai aktivitas kejahatan yang tak tersentuh oleh hukum. Kerugian yang ditimbulkan kejahatan ini dapat bersifat material maupun non-material. *Cybercrime* berpotensi menimbulakan kerugian pada banyak bidang, seperti politik, ekonomi, dan social budaya. Dimasa mendatang kejahatan seperti ini dapat mengganggu prekonomian nasional melalui jaringan infrastruktur yang berbasis teknologi elektronik. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet akan terkena imbas perkembangan *cybercrime* ini. Sehingga sangat dibutuhkan strategi yang tepat untuk menanggulangi *cybercrime* tersebut.

Kata-kata kunci: *Cybercrime. Cyberspace, keamanan system computer, Cyberlaw.*

1. PENDAHULUAN

Kejahatan internet (*cybercrime*) adalah bentuk-bentuk kejahatan yang ditimbulkan karena pemanfaatan teknologi internet, dan dapat didefinisikan sebagai

perbuatan yang melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi computer dan telekomunikasi.

Kejahatan internet sering dilakukan secara transnasional, melintasi batas antar negara sehingga sulit dipastikan yuridiksi hukum negara mana yang diberlakukan. Karakteristik internet dimana orang dapat berlalu lalang tanpa identitas (*anonymous*), hal ini sangat memungkinkan terjadinya berbagai aktivitas kejahatan yang tak tersentuh oleh hukum.

Sifat kejahatan di dunia maya adalah *non-violence*, yaitu tidak menimbulkan kekacauan yang mudah dilihat. Jika kejahatan konvensional sering menimbulkan kekacauan, kejahatan internet malah bersifat sebaliknya. Sehingga ketakutan atas kejahatan (*fear of crime*) tersebut tidak mudah timbul. Meskipum kerusakan yang disebabkannya bisa lebih dahsyat dari kejahatan lain.

Jika pelaku kejahatan konvensional mudah diidentifikasi dan memiliki tipe tertentu, maka pelaku *cybercrime* lebih bersifat universal meskipun memiliki ciri khusus yaitu kejahatan dilakukan oleh orang-orang yang menguasai penggunaan internet beserta aplikasinya. Pelaku kejahatan tidak terbatas pada usia dan *stereotip* tertentu, mereka yang tertangkap ternyata kebanyakan remaja, bahkan ada yang masih anak-anak. Mereka jarang terlibat kenakalan remaja, dari keluarga baik-baik, dan rata-rata cerdas-cerdas. Untuk menangani anak-anak yang seperti ini perlu pendekatan tersendiri.

Keunikan kejahatan ini adalah penggunakan teknologi informasi dalam modus operandi. Itulah sebabnya mengapa modus operandi dalam dunia maya sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan tentang komputer, teknik pemrograman dan sebagainya. Sifat ini yang membuat kejahatan internet berbeda dengan tindak-tindak pidana lainya.

Kerugian yang ditimbulkan kejahatan ini dapat bersifat material maupun non-material, seperti waktu, nilai, jasa, uang, barang, martabat, harga diri, dan bahkan sampai kerahasiaan informasi. Kejahatan internet berpotensi menimbulkan kerugian pada banyak bidang, seperti politik, ekonomi, dan sosial budaya. Dimasa mendatang kejahatan seperti ini dapat mengganggu prekonomian nasional melalui jaringan infrastruktur yang berbasis teknologi elektronik, seperti perbankan, telekomunikasi satelit, jaringan listrik, dan jaringan lalu lintas penerbangan.

2. DEFINISI DAN JENIS-JENIS KEJAHATAN (CYBERCRIME)

Jenis Kejahatan dibedakan mejadi beberapa kategori, yaitu:

A. Berdasarkan Jenis Aktivitasnya

1. *Unauthorized Access*

   Terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Contoh kejahatan ini adalah *probing* dan *port scanning*, aktivitas ini dilakukan untuk melihat servis-servis apa saja yang tersedia di server target.

2. *Illegal Contents*

   Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak etis, tidak benar, dan dapat dianggap melanggar hokum atau menggangu ketertiban umum.

3. Penyebaran Virus dengan Sengaja

   Penyebaran virus umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.

4. Data *Forgery*

   Kejahatan jenis ini bertujuan untuk memalsukan data pada dokumen-dokumen penting yang ada di internet.

5. *Cyber Espionage*, *Sabotage*, dan *Extortion*

   Kejahatan ini merupakan pemanfaatan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki sistem jaringan komputer pihak lain. Selanjutnya *sabotage*, dan *extortion* adalah jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran suatu data, program komputer, atau jaringan komputer yang terhubung ke internet.

6. *Cyberstalking*

   Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer. Misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut merupakan teror yang ditujukan kepada seseorang dengan memanfaatkan internet. Hal ini bias terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

7. *Carding*

   Kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

8. *Hacking* dan *Cracking*

   Istilah *hacking* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Orang yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. *Cracke*r ini sebenarnya adalah *hacker* yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracker* di internet memiliki lingkup yang luas, mulai dari pembajakan *account* milik orang lain, pembajakan situs web, *probing*, penyebaran virus, hingga pelumpuhan target sasaran, sehingga tidak dapat memberikan layanan.

9. *Cybersquatting and Typosquatting*

   Merupakan kejahatan yang dilakukan dengan mendaftarkan *domain* nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. *Typosquatting* adalah kejahatan dengan membuat *domain* yang mirip dengan nama *domain* orang lain.

10. *Hijacking*

    Merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak).

11. *Cyber Terorism*

    Suatu tindakan *cybercrime* termasuk *cyber terorism* jika mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer.

B. **Berdasarkan motif kegiatan yang dilakukan**

1. Kejahatan internet sebagai tindakan murni kriminal

   Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh jenis kejahatan ini adalah *carding*, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfatan media internet (*webserver, mailing list*) untuk menyebarkan material bajakan, dan pengiriman email anonim yang berisi promosi (*spamming*). Para pelaku *spamming* dapat dituntut dengan tuduhan pelanggaran privasi.

2. *Cybercrime* sebagai kejahatan "abu-abu"

   Pada jenis kejahatan di internet yang masuk ke dalam "wilayah abu-abu", cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk berbuat kejahatan.

   Contohnya adalah *probing* atau *portscanning*, yaitu tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, *port-port* yang ada, baik yang terbuka maupun tertutup, dan sebagainya. Kegiatan *cybersquatting* yaitu kejahatan yang berhubungan dengan nama domain di internet. Banyak orang yang melakiukan semacam kegiatan "pencalonan" pada nama domain dengan membeli domain yang mirip dengan merek dagang atau nama perusahaan tertentu dan kemudian menjualnya dengan harga tinggi kepada pemilik merek atau perusahaan yang bersangkutan.

C. Berdasarkan Sasaran Kegiatannya

Sedangkan berdasarkan sasaran kegitannya, *cybercrime* dapat dikelompokkan menjadi beberapa kategori, yakni:

1. Kejahatan internet yang menyerang individu (*Against Person*)

   Kejahatan ini sasaran serangannya ditujukan kepada perorangan yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain:

   - *Pornografi*

     Kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas.

   - *Cyberstalking*

     Kegiatan yang dilakukan untuk mengganggu atau melecehkan dengan memanfaatkan komputer, misalnya dengan menggunakan email yang dilakukan secara berulang-ulang seperti halnya teror di dunia *cyber*.

   - *Cyber-Tresspass*

     Kegiatan yang dilakukan melanggar area privasi orang lain, seperti misalnya *web Hacking*, *breaking ke PC*, *probing*, *Port Scanning*, dan sebagainnya.

2. Kejahatan internet yang menyerang hak milik (*Against Property*)

   Kejahatan yang dilakukan untuk mengganggu atau menyerang milik orang lain. Contonya adalah pengaksesan komputer secara tidak sah melalui dunia *cyber*, pemilikan informasi elektronik secara tidak sah (pencurian informasi), *carding*, *cybersquatting* (mendaftarkan domain nama perusahaan orang lain dan kemudian menjualnya dengan harga yang lebih mahal), *typosquatting* (membuat domain plesetan), *hijacking* (pembajakan hasil karya orang lain), data *forgery* (pemalsuan data) dan segala kegiatan yang bersifat merugikan hal milik orang lain

3. Kejahatan internet yang menyerang pemerintah (*Against Government*)

   Cybercrime Against Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Contohnya *cyber terorism* sebagai

tindakan yang mengancam pemerintah termasuk juga *cracking* ke situs resmi pemerintah atau situs militer.

3. PENANGGULANGAN *CYBERCRIME*

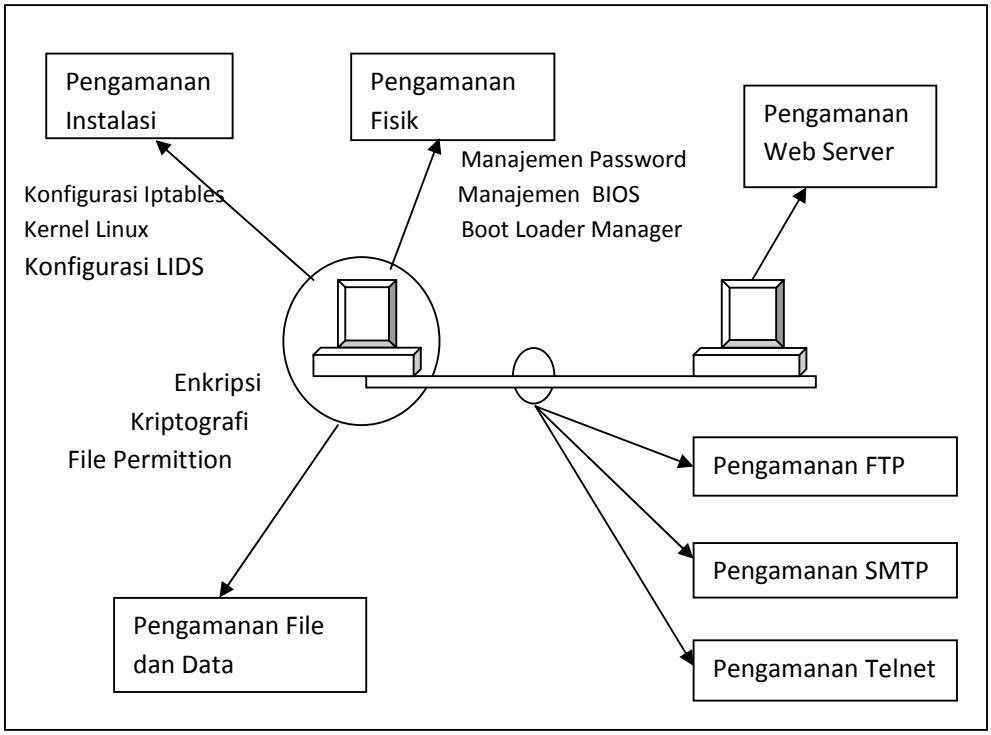
Aktivitas pokok dari kejahatan internet adalah penyerangan terhadap *content*, *computer system* dan *communication system* milik orang lain atau umum di dalam *cyberspace*. Kejahatan internet dapat dilakukan tanpa mengenal batas tritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet akan terkena imbas perkembangan kejahatan internet ini.

Berikut beberapa hal pokok yang dapat dilakukan dalam upaya menanggulangi merebaknya kejahatan internet, yakni:

A. Mengamankan Sistem

Melindungi diri dari kejahatan tersebut dengan mengamankan sistem komputer masing-masing. Pengamanan sistem secara terintegrasi sangat diperlukan untuk meminimalisasi kemungkinan perusakan tersebut. Sistem keamanan yang terintegrasi, berarti berusaha memikirkan segala hal yang dapat menyebabkan celah-celah *unauthorized actions* bersifat merugikan, serta bagaimana cara mengatasi dan meminimalisasi kemungkinan tersebut.

Wahyono (2004) memberikan suatu model keamanan sistem komputer yang terintegrasi seperti gambar berikut:



Gambar: Model keamanan sistem komputer yang terintegrasi

Pengamanan secara personal dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya menuju ke tahap pengamanan fisik dan pengamanan data. Pengamanan akan adanya penyerangan sistem melalui jaringan juga dapat dilakukan dengan melakukan pengamanan FTP, SMTP, Telnet dan pengamanan Web Server.

B. Penanggulangan Global

Saat ini berbagai upaya telah dipersiapkan untuk memerangi kejahatan internet. **The Organization for Economic Coorperation and Development (OECD)** telah membuat guidelines bagi para pembuat kebijakan yang berhubungan dengan *computer-related crime*.

Menurut OECD, berikut beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan kejahatan internet adalah:

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
3. Meningkatkan pemahaman serta keahlian apratur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan kejahatan internet.
4. Meningkatkan kesadaran warga negara mengenai masalah kejahatan internet serta pentingnya mencegah kejahatan tersebut terjadi.
5. Meningkatkan kerjasama antar negara, baik bilateral, regional, maupun multilateral, dalam upaya penanganan *cybercrime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaties*

C. Perlunya Cyberlaw

Dengan adanya kejahatan-kejahatan dan kendala-kendala hukum bidang teknologi informasi saat ini telah lahir suatu rezim hukum baru yang dikenal dengan

Hukum Siber. Istilah hukum siber diartikan sebagai padanan kata dari *Cyber Law*, yang saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Optimalisasi peranan hukum dalam perkembanngan teknologi membutuhkan kelengkapan perundang-undangan yang berkualitas. Misalnya memperluas pengertian "barang" secara konvensional sehingga mencakup data, program, atau jasa computer dan telekomunikasi. Pengertian "surat" yang selama ini hanya dibedakan atas surat akta dan bukan akta , diperluas mencakup data yang tersimpan dalam pita magnetic, disket dan lain sebagainya.

D. Perlunya Dukungan Lembaga Khusus

Lembaga-lembaga khusus, baik milik pemerintah maupun NGO (*Non Government Organization*), diperlukan sebagai upaya penanggulangan kejahatan di internet. Amerika Serikat memiliki *Computer Crime and Intellectual Property Section (CCIPS)* sebagai sebuah divisi khusus dari U.S. Departement of Justice. Institusi ini memberikan informasi tentang kejahatan internet, melakukan sosialisasi secar intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan kejahatan internet .

Indonesia sendiri sudah memiliki IDCERT (*Indonesia Coputer Emergency Response Team*). Unit ini merupakan *point of contact* bagi orang untuk melaporkan masalah-masalah keamanan computer.

4. KESIMPULAN

Permasalahan yang sering muncul adalah bagaimana menjaring berbagai kejahatan komputer dikaitkan dengan ketentuan pidana yang berlaku, Karena ketentuan pidana yang mengatur tentang kejahatan computer yang berlaku saat ini masih belum lengkap. Untuk optimalisasi peranan hukum dalam perkembangan teknologi sangat dibutuhkan kelengkapan perundang-undangan yang berkualitas. Misalnya memperluas pegertian "barang" secara konvensional sehingga mencakup data, program, atau jasa computer dan telekomunikasi. Pengertian "surat" yng selama ini hanya dibedakan atas surat akta dan bukan akta diperluas mencakup data yang tersimpan dalam pita *magnetic*, disket dan lain sebagainya. Dampak negatif yang serius karena berkembangnya teknologi informasi terutama teknologi internet harus segera ditangani dan ditanggulangi dengan segala perangkat yang mungkin, termasuk perangkat perundangan yang bisa mengendalikan kejahatan dibidang teknologi

informasi. Sudah saatnya bahwa hukum yang ada harus bisa mengatasi penyimpangan penggunaan perangkat teknologi informasi sebagai alat bantunya, terutama kejahatan di internet (*cybercrime*) dengan menerapkan hukum siber (*cyberlaw*), yang saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi..

5. DATAR PUSTAKA

[1]. Wahyono, Teguh (2006), Etika Komputer dan Tanggung Jawab Profesional di bidang Teknologi Informasi, Penerbit ANDI, Yogyakarta.

[2]. Wahyono, Teguh (2004), Membangun Keamanan yang Terintegrasi pada Sistem Komputer Berbasis Linux, Penerbit FTI UKSW, Salatiga.