KEJAHATAN DALAM TEKNOLOGI INFORMASI DAN KOMUNIKASI

Dodo Zaenal Abidin
Program Studi Sistem Informasi, STIKOM Dinamika Bangsa
Jl. Jend. Sudirman, Thehok, Jambi
Email : dodozaenal@yahoo.com

ABSTRAK

Perkembangan teknologi jaringan komputer global atau Internet telah menciptakan dunia baru yang dinamakan cyberspace. Cyberspace menghasilkan berbagai bentuk lingkungan cyberspace yang kemudian melahirkan istilah baru yang dikenal dengan Cybercrime. Cybercrime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Cybercrime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Jenis-jenis cybercrime terbagi menjadi tiga macam, yaitu berdasarkan aktifitas yang dilakukannya, motif kegiatan, dan sasaran kejahatan.

Kata Kunci : Ancaman dan Teknologi Informasi, Kejahatan, Cyberspace, Cybercrime.

ABSTRACT

Development of technology on a global computer network or the Internet has created a new world called cyberspace. Cyberspace produces various forms of environmental cyberspace which later gave birth to a new term known as Cybercrime. Cybercrime iscrime-shapes that arise due to the utilization ofinternet technology. Cybercrime is formulated as atort committed using computer networks as a means/tools or computer as objects, whether forprofit or not, with the detriment of the other party.Types of cybercrime is divided into three kinds,namely based on activities that it does, the motiveactivity, and target crime.

Keywords: threats and information technology, crime,Cyberspace, Cybercrime.

1. PENDAHULUAN

Perkembangan teknologi informasi-komputer saat ini sudah mencapai pada tahap di mana ukurannya semakin kecil, kecepatannya semakin tinggi, namun harganya semakin murah dibandingkan dengan kemampuan kerjanya. Hal ini yang menyebabkan kebutuhan akan teknologi jaringan komputer semakin meningkat. Perkembangan teknologi jaringan komputer global atau Internet telah menciptakan dunia baru yang dinamakan *cyberspace*, sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru, yaitu realitas virtual. Banyak segi positif yang dapat diambil dari dunia maya ini, diantaranya dapat dengan mudah mendapatkan informasi, melakukan transaksi jual-beli secara *online*, menambah lingkup pertemanan dengan social media secara online, dan tentu saja menambah trend perkembangan teknologi dunia dengan segala krestifitas manusia. Jika ada segi positif tentu saja ada segi negatifnya, salah satunya seperti pornografi. Namun, teknologi yang semakin berkembang juga membuat segi negatif semakin bertambah, yaitu dengan munculnya istilah kejahatan internet. *Cyberspace* menghasilkan berbagai bentuk lingkungan cyberspace yang kemudian melahirkan istilah baru yang dikenal dengan *Cybercrime*, Internet Fraud, dan lain-lain. *Cybercrime* atau kejahatan melalui jaringan internet saat ini semakin tak terbendung. Di Indonesia, kejahatan ini dilakukan untuk pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer. Adanya Cybercrime telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

Kebutuhan akan teknologi Jaringan Komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui Internet pula kegiatan komunitas komersial menjadi bagian terbesar, dan terpesat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar di dunia bisa diketahui selama 24 jam. Melalui dunia internet atau disebut juga cyberspace, apapun dapat

dilakukan. Segi positif dari dunia maya ini tentu saja menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Namun dampak negatif pun tidak bisa dihindari. Tatkala pornografi marak di media Internet, masyarakat pun tak bisa berbuat banyak.

2. PEMBAHASAN

Semakin maraknya tindakan kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini semakin membuat para kalangan pengguna jaringan telekomunikasi menjadi resah. Beberapa jenis kejahatan atau ancaman (threats) yang dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada.

Pengertian *Cybercrime*

Cybercrime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Beberapa pendapat mengindentikkan *cybercrime* dengan *computer crime.* **The U.S. Department of Justice** memberikan pengertien *computer crime* sebagai:

"*…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution".*

(www.usdoj.gov/criminal/cybercrimes)

Pengertian tersebut identik dengan yang diberikan **Organization of European Community Development**, yang mendefinisikan *computer crime* sebagai:

"any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data".

Adapun Andi Hamzah (1989) dalam tulisannya "Aspek-aspek Pidana di Bidang komputer", mengartikan kejahatan komputer sebagai:

"Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal".

Dari beberapa pengertian di atas, secara ringkas dapat dikatakan bahwa *cybercrime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

A. Karakteristik Cybercrime

Selama ini dalam kejahatan konvensional, dikenal adanya dua jenis kejahatan sebagai berikut:

1. **Kejahatan kerah biru (blue collar crime)**
   Kejahatan ini merupakan jenis kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti misalnya perampokkan, pencurian, pembunuhan dan lain-lain.
2. **Kejahatan kerah putih (white collar crime)**
   Kejahatan jenis ini terbagi dalam empat kelompok kejahatan, yakni kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu.

Cybercrime sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik tersendiri yang berbeda dengan kedua model di atas. Karakteristik unik dari kejahatan di dunia maya tersebut antara lain menyangkut lima hal berikut:

1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Pelaku kejahatan
4. Modus Kejahatan
5. Jenis kerugian yang ditimbulkan

B. Jenis Cybercrime

Berdasarkan jenis aktifitas yang dilakukannya, cybercrime dapat digolongkan menjadi beberapa jenis sebagai berikut:

1. **Unauthorized Access**
   Merupakan kejahatan yang 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. *Probing* dan *port* merupakan contoh kejahatan ini.

2. Illegal Contents

Merupakan kejahatn yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.

3. Penyebaran virus secara sengaja

Penyebaran virus pada 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 dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.

5. Cyber Espionage, Sabotage, and Extortion

Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. *Sabotage and Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan 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 menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

7. Carding

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

8. Hacking dan Cracker

Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

9. Cybersquatting and Typosquatting

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

10. Hijacking

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. Beberapa contoh kasus Cyber Terorism sebagai berikut :

- Ramzi Yousef, dalang penyerangan pertama ke gedung WTC, diketahui menyimpan detail serangan dalam file yang di enkripsi di laptopnya.
- Osama Bin Laden diketahui menggunakan steganography untuk komunikasi jaringannya.
- Suatu website yang dinamai Club Hacker Muslim diketahui menuliskan daftar tip untuk melakukan hacking ke Pentagon.
- Seorang hacker yang menyebut dirinya sebagai DoktorNuker diketahui telah kurang lebih lima tahun melakukan defacing atau mengubah isi halaman web dengan propaganda anti-American, anti-Israel dan pro-Bin Laden.

C. Berdasarkan Motif Kegiatan

Berdasarkan motif kegiatan yang dilakukannya, cybercrime dapat digolongkan menjadi dua jenis sebagai berikut :

1. Cybercrime sebagai tindakan murni kriminal

Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah *Carding*, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (webserver, mailing list) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (*spamming*) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku spamming dapat dituntut dengan tuduhan pelanggaran privasi.

2. Cybercrime sebagai kejahatan ”abu-abu”

Pada jenis kejahatan di internet yang masuk dalam wilayah ”abu-abu”, cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah sebutan untuk semacam 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.

D. Berdasarkan Sasaran Kejahatan

Sedangkan berdasarkan sasaran kejahatan, cybercrime dapat dikelompokkan menjadi beberapa kategori seperti berikut ini :

1. Cybercrime yang menyerang individu (Against Person)

Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu 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 seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia cyber. Gangguan tersebut bisa saja berbau seksual, religius, dan lain sebagainya.
- ***Cyber-Tresspass***
  Kegiatan yang dilakukan melanggar area privasi orang lain seperti misalnya Web Hacking. Breaking ke PC, Probing, Port Scanning dan lain sebagainya.

2. Cybercrime menyerang hak milik (*Againts Property*)

Cybercrime yang dilakukan untuk menggangu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia cyber, pemilikan informasi elektronik secara tidak sah/pencurian informasi, carding, cybersquating, hijacking, data forgery dan segala kegiatan yang bersifat merugikan hak milik orang lain.

3. Cybercrime menyerang pemerintah (*Againts Government*)

Cybercrime Againts Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya *cyber terorism* sebagai tindakan yang mengancam pemerintah termasuk juga cracking ke situs resmi pemerintah atau situs militer.

E. Penanggulangan Cybercrime

Aktivitas pokok dari *cybercrime* adalah penyerangan terhadap content, computer system dan communication system milik orang lain atau umum di dalam cyberspace. Fenomena cybercrime memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. Cybercrime dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan. Berikut ini cara penanggulangannya :

1. Mengamankan sistem

Tujuan yang nyata dari sebuah sistem keamanan adalah mencegah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem secara terintegrasi sangat diperlukan untuk meminimalisasikan kemungkinan perusakan tersebut. Membangun sebuah keamanan sistem harus merupakan langkah-langkah yang terintegrasi pada keseluruhan subsistemnya, dengan tujuan dapat mempersempit atau bahkan menutup adanya celah-celah unauthorized actions yang merugikan. Pengamanan secara personal dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya menuju ke tahap pengamanan fisik dan pengamanan data. Pengaman akan adanya penyerangan sistem melaui jaringan juga dapat dilakukan dengan melakukan pengamanan FTP, SMTP, Telnet dan pengamanan Web Server.

2. Penanggulangan Global

The Organization for Economic Cooperation and Development (OECD) telah membuat guidelines bagi para pembuat kebijakan yang berhubungan dengan computer-related crime, dimana pada tahun 1986 OECD telah memublikasikan laporannya yang berjudul Computer-Related Crime : *Analysis of Legal Policy*. Menurut OECD, beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime adalah :

- Melakukan modernisasi hukum pidana nasional beserta hukum acaranya.
- Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
- Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*.
- meningkatkan kesadaran warga negara mengenai masalah *cybercrime* serta pentingnya mencegah kejahatan tersebut terjadi.
- meningkatkan kerjasama antarnegara, baik bilateral, regional maupun *multilateral*, dalam upaya penanganan *cybercrime*.

F. Karakteristik unik Kejahatan bidang TI

1. Ruang Lingkup kejahatan

Bersifat global (melintasi batas negara) menyebabkan sulit menentukan yuridiksi hukum negara mana yang berlaku terhadapnya Sifat Kejahatan Tidak menimbulkan kekacauan yang mudah terlihat (non-violence), sehingga ketakutan terhadap kejahatan tersebut tidak mudah timbul.

2. Pelaku Kejahatan

Pelaku kejahatan ini tidak mudah didentifikasi, namun memiliki ciri khusus yaitu pelakunya menguasai penggunaan internet / komputer.

3. Modus Kejahatan

Modus kejahatan hanya dapat dimengerti oleh orang yang mengerti dan menguasai bidang teknologi informasi.

3. Jenis Kerugian

Kerugian yang ditimbulkan lebih luas, termasuk kerugian dibidang politik, ekonomi, sosial dan budaya.

G. Gambaran Umum Perkembangan Kejahatan Komputer (*Cybercrime*) di Indonesia

Di Indonesia pada Januari 2000, beberapa situs di Indonesia diacak – acak oleh *cracker* yang menamakan dirinya " Fabian Clone " dan " naisedoni " (" Indonesia " dibaca dari belakang). Situs yang diserang termasuk Bursa Efek Jakarta, BCA, Indosatnet. Selain situs yang besar tersebut masih banyak situs lainnya yang tidak dilaporkan. Selanjutnya pada tahun yang sama seorang *cracker* Indonesia tertangkap di Singapura ketika mencoba menjebol sebuah perusahaan di Singapura. Pada bulan September dan Oktober 2000, setelah berhasil membobol Bank Lippo, kembali Fabian Clone beraksi dengan menjebol web milik Bank Bali. Perlu diketahui bahwa kedua bank ini memberikan layanan perbakan internet *(Internet Banking)*.

Bulan September 2000, polisi mendapat banyak laporan dari luar negeri tentang adanya pengguna Indonesia yang mencoba menipu pengguna lain pada situs web yang menyediakan transaksi lelang *(auction)* seperti eBay. Kemudian pada tanggal 24 Oktober 2000, dua warung internet (warnet) di Bandung digerebak oleh Polisi dikarenakan mereka menggunakan account dialup curian dari ISP Centrin. Salah satu dari warnet tersebut sedang online dengan menggunakan *account* curian tersebut. Juni 2001 Seorang pengguna internet Indonesia membuat beberapa situs yang mirip dengan situs klikbca.com, yang digunakan oleh BCA untuk memberikan layanan perbankan internet. Situs yang dibuat menggunakan nama domain yang mirip dengan klikbca.com, dan masih banyak lagi contoh yang lain.

Perusahaan MarkPlus Co telah melakukan survey yang kemudian dimuat pada majalah Swa Sembada (disi No.11/XVI/30 Mei – 12 Juni 2001) data dijadikan rujukan. Survey itu sendiri dilakukan pada 22 Maret 2000 hingga 5 April 2000 dengan mengambil responden sebanyak 1100 orang dari 5 kota Utama di Indonesia, yaitu Jabodetabek 250 orang, Bandung 200 orang, Yogyakarta 150 orang, Surabaya 200 orang, dan Medan 100 orang. Dari data – data yang dikumpulkan dari para responden tersebut, tergambarkan bahwa 14,2 % responden mulai menggunakan Internet kurang dari 6 bulan yang lalu, 25,9% antara 6 – 12 bulan yang lalu, 31,3% antara 1 – 2 tahun yang lalu, 13,7% antara 2 – 3 tahun yang lalu, 8,4% antara 3- 4 tahun yang lalu dan 6,6% merupakan pengguna yang telah menggunakan Internet lebih dari 4 tahun yang lalu. Hal yang perlu digarisbawahi pada hasil survey tersebut adalah 90,1% tidak pernah merasa tidak aman / beresiko tinggi (13,6 %). Ini berarti lebih drai 25% dari 1100 responden enggan bertransaksi e–commerce karena kuatir dengan faktor keamanan bertransaksi melalui internet.

Dampak kejahatan kartu kredit yang dilakukan lewat transaksi online, oleh *carder* orang Indonesia, membuat beberapa merchant online di AS dan Australia sudah memasukkan Indonesia ke dalam daftar hitam mereka. Bahkan ada dugaan kuat, FBI tengah menjadikan beberapa kota di Indonesia sebagai sasaran pengawasan langsung. Hal ini terjadi karena *carder*, ada yang menyejajarkannya dengan *hacker* dan *cracker*, merugikan beberapa pihak asing, seperti yang terjadi di Yogyakarta. Polda Daerah Istimewa Yogyakarta menangkap lima carder dan mengamankan barang bukti bernilai puluhan juta, yang didapat dri merchant luar negeri.

Riset juga pernah dilakukan oleh perusahaan sekuritas *ClearCommerce* (Clearcommerce.com) yang bermarkas di Texas, Amerika Serikat. Menurut data riset tersebut, 20% dari total transaksi kartu kredit dari Indonesia di internet adalah *fraud* (bohong). Tidak heran jika kondisi itu semakin memperparah sektor bisnis di dalam negeri, khususnya yang memanfaatkan teknologi informasi. Berdasarkan hasil survey CasteAsia (CastleAsia.com) yang dilansir pda bulan Januari 2002, ditunjukkan bahwa hanya 15% responden Usaha Kecil dan Menengah (UKM) di Indonesia yang bersedia menggunakan perbankan internet. Dari 85% sisanya, setengahnya beralasan khawatir dengan keamanan transaksi di internet.

Berita Kompas Cyber Media (19/3/2002) menulis bahwa berdasarkan survey AC Nielsen 2001 Indonesia ternyata menempati posisi keenam terbesar di dunia atau keempat di Asia dalam tindak kejahatan di internet. Meski tidak disebutkan secara rinci kejahatan macam apa saja yang terjadi di Indonesia maupun WNI yang terlibat dalam kejahatan tersebut, hal ini merupakan peringatan bagi semua pihak untuk mewaspadai kejahatan yang telah, sedang, dan akan muncul dari pengguna teknologi informasi (Heru Sutadi, Kompas, 12 April 2002).

Tahun 2004 di Indonesia juga dihebohkan jebolnya komputer server Komisi Pemilihan Umum yang dibobol oleh *spyware* berasal dari Indonesia bernama Dani Firmansyah, yang akhirnya mengacaukan sistem yang ada di KPU. Mulanya ia mengetes sistem sistem keamanan server www.tnp.kpu.go.id melalui *Cross Site Scripting* (XSS) dan SQL Injection di gedung PT Danareksa Jln. Medan Merdeka Selatan, Jakarta Pusat pada 17 April 2004. Usahanya sukses, selanjutnya ia berbuat iseng dengan mengubah nama – nama partai dengan istilah – istilah yang lucu. Seperti Partai Kolor Ijo, Partai Jambu, Partai Nanas, dan lain – lain.

Dari sebagian data tersebut terlihat bahwa tingginya angka *cybercrime* di Indonesia akan berpengaruh secara langsung pada sektor bisnis skala kecil, menengah dan besar. Pengaruh dunia dan komunitas bisnis secara umum.

H. Hukum yang Mengatur Kejahatan Komputer di Indonesia

Pemerintah Indonesia baru saja mengatur masalah HaKI (Hak atas Kekayaan Intelektual), Undang – Undang Nomor 19 Tahun 2002. Namun undang – undang tersebut berfokus pada persoalan perlindungan kekayaan intelektual saja. Ini terkait dengan persoalan tingginya kasus pembajakan software di negeri ini. Kehadiran undang – undang tersebut tentu tidak lepas dari desakan Negara – Negara dimana produsen software itu berasal. Begitu juga dengan dikeluarkannya undang – undang hak paten yang diatur dalam Undang – Undang Nomor 14 Tahun 2001, yang mengatur hak eksklusif yang diberikan oleh Negara kepada inventor atas hasil invensinya di bidang teknologi, yang untuk selama waktu tertentu melaksanakan sendiri Invensinya tersebut atau memberikan persetujuannya kepada pihak lain untuk melaksanakannya.

Terlepas dari masalah itu, sebenarnya kehadiran *cyberlaw* yang langsung memfasilitasi *e–commerce*, *e–government*, dan *cybercrime* sudah sangat diperlukan. Menurut Yappi Manafe, Asisten Deputi Urusan Perundangan Telematika pada Kementerian Komunikasi dan Informasi, ketiga materi tersebut dicakup dalam RUU Informasi dan Transaksi Elektronik (ITE). Pengakomodasian ketiga materi tersebut dirasakan sudah sangat mendesak mengingat persoalan ketiganya memang sudah muncul dalam kehidupan secara nyata.

Dalam RUU Pemanfaatan teknologi kegiatan yang diatur meliputi :

- Perdagangan elektronik (e–commerce)
- Perbankan elektronik (e–banking)
- Pemerintahan elektronik (e–government)
- Pelayanan kesehatan elektronik (e–hospital)
- Pemberian nama domain (Domain Name Servises – DNS)

I. Perlunya Cyberlaw

Perkembangan teknologi yang sangat pesat, membutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut. Sayangnya, hingga saat ini banyak negara belum memiliki perundang-undangan khusus di bidang teknologi informasi, baik dalam aspek pidana maupun perdatanya.

Permasalahan yang sering muncul adalah bagaimana menjaring berbagai kejahatan komputer dikaitkan dengan ketentuan pidana yang berlaku karena ketentuan pidana yang mengatur tentang kejahatan komputer yang berlaku saat ini masih belum lengkap.

Banyak kasus yang membuktikan bahwa perangkat hukum di bidang TI masih lemah. Seperti contoh, masih belum dilakuinya dokumen elektronik secara tegas sebagai alat bukti oleh KUHP. Hal tersebut dapat dilihat pada UU No8/1981 Pasal 184 ayat 1 bahwa undang-undang ini secara definitif membatasi alat-alat bukti hanya sebagai keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa saja. Demikian juga dengan kejahatan pornografi dalam internet, misalnya KUH Pidana pasal 282 mensyaratkan bahwa unsur pornografi dianggap kejahatan jika dilakukan di tempat umum.

Hingga saat ini, di negara kita ternyata belum ada pasal yang bisa digunakan untuk menjerat penjahat *cybercrime*. Untuk kasuss carding misalnya, kepolisian baru bisa menjerat pelaku kejahatan komputer dengan pasal 363 soal pencurian karena yang dilakukan tersangka memang mencuri data kartu kredit orang lain.

J. 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 komputer *Crime and Intellectual Property Section* (CCIPS) sebagai sebuah divisi khusus dari U.S. Departement of Justice. Institusi ini memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime. Indonesia sendiri sebenarnya sudah memiliki IDCERT (*Indonesia Computer Emergency Rensponse Team*). Unit ini merupakan *point of contact* bagi orang untuk melaporkan masalah-masalah keamanan komputer.

L. Contoh Kasus Kejahatan Cyber Crime

1. Membajak situs web Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di Indonesia menunjukkan satu (1) situs web dibajak setiap harinya.
2. Probing dan port scanning Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan port scanning atau probing untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya.
3. Virus Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia . Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, I love you, dan SirCam. Untuk orang yang terkena virus, kemungkinan tidak banyak yang dapat kita lakukan.
4. Denial of Service (DoS) dan Distributed DoS (DDos) attack DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial.

3. KESIMPULAN

Kejahatan komputer yang banyak terjadi seperti menjadi "momok" bagi para pengguna. Maka, untuk memperkecil angka kejahatan komputer dibutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut. Namun, hingga saat ini banyak negara belum memiliki perundang-undangan khusus di bidang teknologi informasi, baik dalam aspek pidana maupun perdatanya.

Semakin meningkatnya Teknologi Informasi semakin banyak juga dampak positif dan negatifnya. Segi positif dari dunia maya ini tentu saja menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Selain itu dampak negatifnya dapat menyebabkan munculnya kejahatan yang disebut dengan "CyberCrime" atau kejahatan melalui jaringan Internet. Semakin maraknya tindakan kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini semakin membuat para kalangan pengguna jaringan telekomunikasi menjadi resah.

DAFTAR PUSTAKA

[1] Irhamni Ali. *Kejahatan Terhadap Informasi (Cybercrime) Dalam Konteks Perpustakaan Digital*. IPB. 2011.

[2] Suryo Widiantoro. *Modus Kejahatan Dalam Teknologi Informasi*. UBM. 2009

[3] https://balianzahab.wordpress.com/cybercrime/modus-modus-kejahatan-dalam-teknologi-informasi/, diambil 3 Oktober 2015.