

## Kriminalitas di Internet (Cybercrime)

Kriminalitas dunia maya (*cybercrime*) atau kriminalitas di internet adalah tindakan pidana kriminal yang dilakukan pada teknologi internet (*cyberspace*), baik yang menyerang fasilitas umum di dalam *cyberspace* ataupun kepemilikan pribadi. Secara teknik tindak pidana tersebut dapat dibedakan menjadi *off-line crime*, *semi on-line crime*, dan *cybercrime*. Masing-masing memiliki karakteristik tersendiri, namun perbedaan utama antara ketiganya adalah keterhubungan dengan jaringan informasi publik (internet).

## Motif Kejahatan di Internet

- **Motif intelektual**, yaitu kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya telah mampu untuk merekayasa dan mengimplementasikan bidang teknologi informasi.
- **Motif ekonomi, politik, dan kriminal**, yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain.

## Faktor Penyebab Cybercrime

- **Segi teknis**, adanya teknologi internet akan menghilangkan batas wilayah negara yang menjadikan dunia ini menjadi begitu dekat dan sempit. Saling terhubungnya antara jaringan yang satu dengan jaringan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya. Kemudian, meratanya penyebaran teknologi menjadikan yang satu lebih kuat daripada yang lain.
- **Segi sosioekonomi**, adanya *cybercrime* merupakan produk ekonomi. Isu global yang kemudian dihubungkan dengan kejahatan tersebut adalah keamanan jaringan (*security network*) keamanan jaringan merupakan isu global yang muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. *Cybercrime* berada dalam skenario besar dari kegiatan ekonomi dunia. Sebagai contoh saat ini, memasuki tahun 2000 akan terjadi berupa isu virus Y2K yang akan menghilangkan atau merusak data atau informasi. Hal tersebut tentu saja membuat kekhawatiran terhadap usaha perbankan, penerbangan, pasar modal, dan sebagainya, yang pada akhirnya mereka sibuk mencari solusi cara menghindarinya. Sehingga hal tersebut menjadi ladang para penyedia jasa teknologi informasi untuk membuat perangkat atau program untuk menangulangnya, yang pada akhirnya kenyataannya ancaman tersebut tidak pernah terjadi.

## Empat Ruang Lingkup Kejahatan Komputer

1. **Komputer sebagai instrumen untuk melakukan kejahatan tradisional**, seperti digunakan untuk melakukan pencurian, penipuan, dan pemalsuan melalui internet, di samping kejahatan lainnya seperti pornografi terhadap anak-anak, prostitusi online, dan lain-lain.
2. **Komputer dan perangkatnya sebagai objek penyalahgunaan**, di mana data-data di dalam komputer yang menjadi objek kejahatan dapat saja diubah, dimodifikasi, dihapus, atau duplikasi secara tidak sah.
3. **Penyalahgunaan yang berkaitan dengan komputer atau data**, yang dimaksud dengan penyalahgunaan di sini yaitu manakala komputer dan data-data yang terdapat di dalam komputer digunakan secara ilegal atau tidak sah.
4. **Unauthorized acquisition, disclosure or use of information and data**, yang berkaitan dengan masalah penyalahgunaan hak akses dengan cara-cara yang ilegal.

Kejahatan menggunakan sarana komputer  
(Bainbridge, 1993) :

1. Memasukkan instruksi yang tidak sah;
2. Perubahan data input;
3. Perusakan data;
4. Komputer sebagai pembantu kejahatan;
5. Akses tidak sah terhadap sistem komputer.

Ancaman terhadap Penggunaan Internet  
(Bernstein et.al., 1996):

1. **Menguping** (*eavesdropping*);
2. **Menyamar** (*masquerade*);
3. **Pengulang** (*reply*);
4. **Manipulasi data** (*data manipulation*);
5. **Kesalahan Penyampaian** (*misrouting*);
6. **Pintu jebakan atau kuda Trojan** (*trapdoor*);
7. **Virus** (*viruses*);
8. **Pengingkaran** (*repudiation*);
9. **Penolakan Pelayanan** (*denial of service*).

Beberapa kendala di internet akibat lemahnya  
sistem keamanan komputer (Bernstein et.al.,  
1996):

1. Kata sandi seseorang dicuri ketika terhubung ke sistem jaringan dan ditiru atau digunakan oleh pencuri.
2. Jalur komunikais disadap dan rahasia perusahaan pun dicuri melalui jaringan komputer.
3. Sistem informasi dimasuki (*penetrated*) oleh pengacau (*intruder*).
4. Server jaringan dikirim data dalam ukuran sangat besar (*e-mail bomb*) sehingga sistem macet.

Masalah keamanan berhubungan  
dengan lingkungan hukum:

1. Kekayaan intelektual (*intellectual property*) dibajak.
2. Hak cipta dan paten dilanggar dengan melakukan peniruan dan atau tidak membayar royalti.
3. Terjadi pelanggaran terhadap ketentuan penggunaan teknologi tertentu.
4. Dokumen rahasia disiarkan melalui *mailing list* atau *bulletin boards*.
5. Pegawai menggunakan internet untuk tindakan asusila seperti pornografi.

### Sistem keamanan yang berkaitan dengan masalah keuangan dan *e-commerce*:

1. Data keuangan dapat dicuri atau diubah oleh intruder atau *hacker*;
2. Dana atau kas disalahgunakan oleh petugas yang memegangnya;
3. Pemalsuan uang;
4. Seseorang dapat berpura-pura sebagai orang lain dan melakukan transaksi keuangan atas nama orang lain tersebut.

### Tipenya *cybercrime* menurut Philip Renata:

1. *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin.
2. *Hacking*, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.
3. *The trojan horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau, dengan tujuan kepentingan pribadi atau orang lain.
4. *Data leakage*, yaitu menyangkut pembocoran data ke luar terutama mengenai data yang harus dirahasiakan.
5. *Data diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah input data atau output data.
6. *To frustate data communication* atau penyia-nyiaan data komputer.
7. *Software piracy*, yaitu pembajakan software terhadap hak cipta yang dilindungi Hak atas Kekayaan Intelektual (HaKI).

### Bentuk kejahatan yang berhubungan erat dengan penggunaan TI:

1. Unauthorized Access to Computer System and Service;
2. Illegal Contents;
3. Data Forgery;
4. Cyber Espionage;
5. Cyber Sabotage and Extortion;
6. Offense Against Intellectual Property;
7. Infringement of Privacy.

### Modus Kejahatan Cybercrime Indonesia (Roy Suryo):

- Pencurian nomor kredit;
- Memasuki, memodifikasi, atau merusak homepage (hacking);
- Penyerangan situs atau e-mail melalui virus atau spamming.

### Kasus Cybercrime yang sering Terjadi di Indonesia (As'ad Yusuf):

1. Pencurian nomor kartu kredit;
2. Pengambilalihan situs web milik orang lain;
3. Pencurian akses internet yang sering dialami oleh ISP;
4. Kejahatan nama domain;
5. Persaingan bisnis dengan menimbulkan gangguan bagi situs saingannya.