CYBERCRIME

Kriminalitas di Internet

- 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.

- Cybercrime → perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis kecanggihan teknologi komputer dan telekomunikasi.

Motif

- Motif intelektual

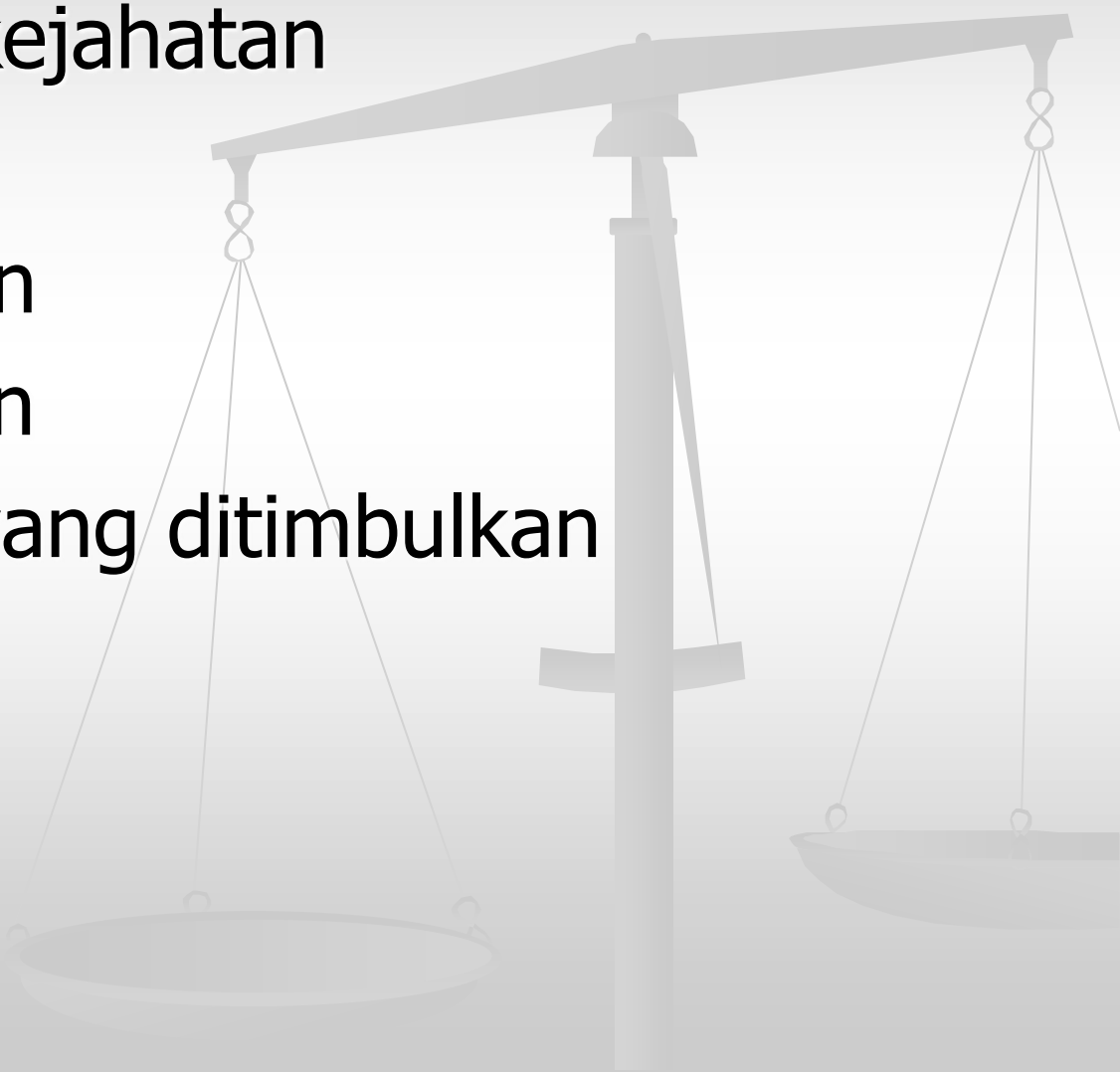
  Kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya telah mampu untuk merekayasa dan mengimplementasikan bidang teknologi informasi.

- Motif ekonomi, politik, dan kriminal

  Kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain.

Karakteristik cybercrime

- Ruang lingkup kejahatan
- Sifat kejahatan
- Pelaku kejahatan
- Modus kejahatan
- Jenis kerugian yang ditimbulkan



Karakteristik cybercrime

- Ruang lingkup kejahatan

  → Bersifat global

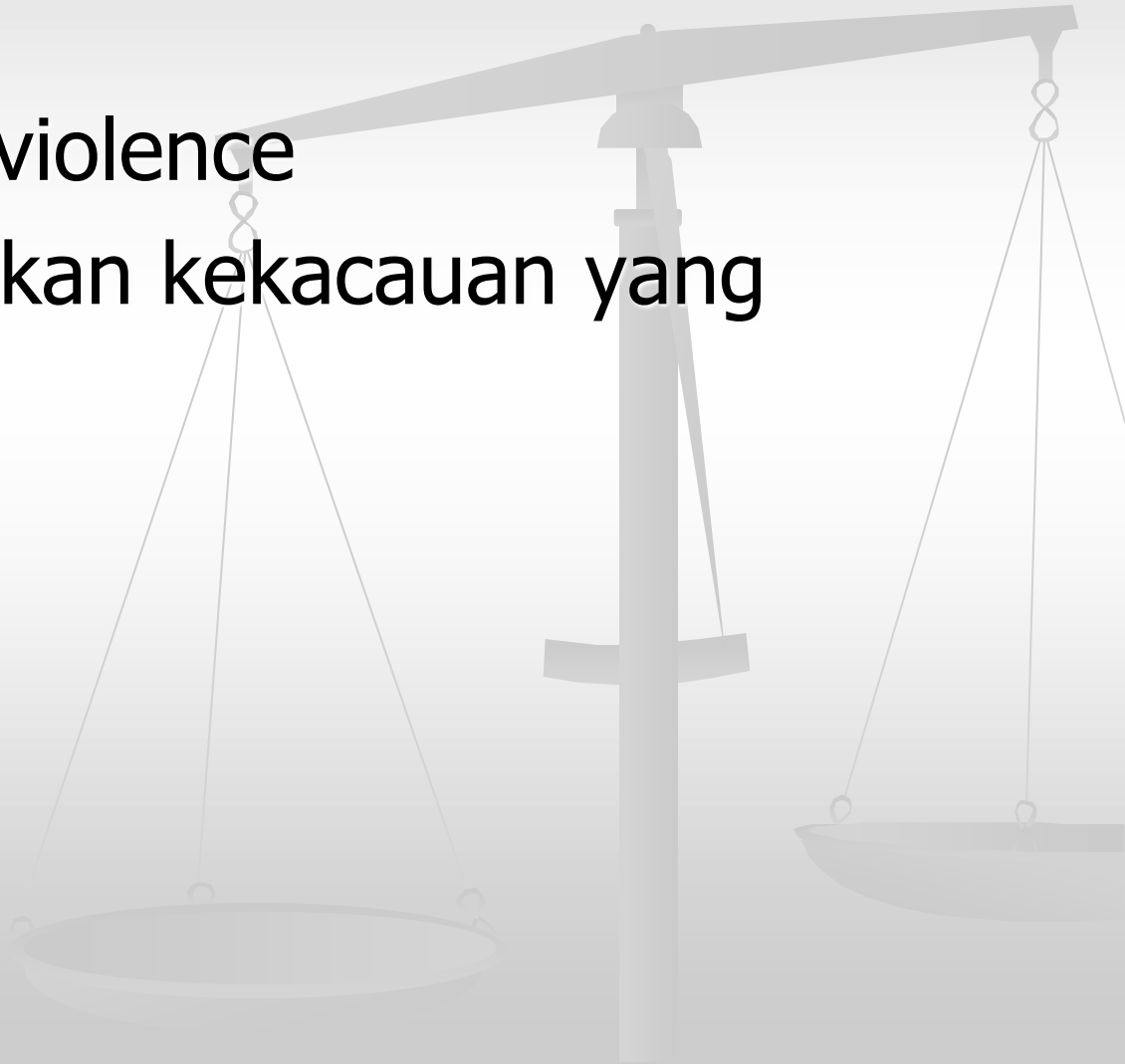
  Cybercrime seringkali dilakukan secara transnasional, melintasi batas negara sehingga sulit dipastikan yuridikasi hukum negara yang berlaku terhadap pelaku. Karakteristik internet di mana orang dapat berlalu-lalang tanpa identitas (anonymous) memungkinkan terjadinya berbagai aktivitas jahat yang tak tersentuh hukum.

Karakteristik cybercrime

- Sifat kejahatan

  → Bersifat non-violence

  Tidak menimbulkan kekacauan yang mudah terlihat.



Karakteristik cybercrime

- Pelaku kejahatan

  → Bersifat lebih universal

  Kejahatan dilakukan oleh orang-orang yang menguasai penggunaan internet beserta aplikasinya.

Karakteristik cybercrime

- Modus kejahatan

  Keunikan kejahatan ini adalah penggunaan teknologi informasi dalam modus operandi, sehingga sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan tentang komputer, teknik pemrograman dan seluk beluk dunia cyber.

Karakteristik cybercrime

- Jenis kerugian yang ditimbulkan

  → Dapat bersifat material maupun non-material

  Waktu, nilai, jasa, uang, barang, harga diri, martabat bahkan kerahasiaan informasi.

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 diduplikasi secara tidak sah.

Ruang Lingkup Kejahatan Komputer

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** (*repudoition*);
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*:

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

Faktor Penyebab Cybercrime

- ***Segi teknis***,

  Teknologi internet 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, tidak meratanya penyebaran teknologi menjadikan yang satu lebih kuat daripada yang lain.

Faktor Penyebab Cybercrime

- ***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 skenerio besar dari kegiatan ekonomi dunia. Sebagai contoh, memasuki tahun 2000 terjadi 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 menanggulanginya, yang pada akhirnya kenyataannya ancaman tersebut tidak pernah terjadi.

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 intsruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau, dengan tujuan kepentingan pribadi atau orang lain.

Tipenya *cybercrime* menurut Philip Renata:

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).

Modus Kejahatan Cybercrime Indonesia (Roy Suryo):

- Pencurian nomor (kartu) 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):

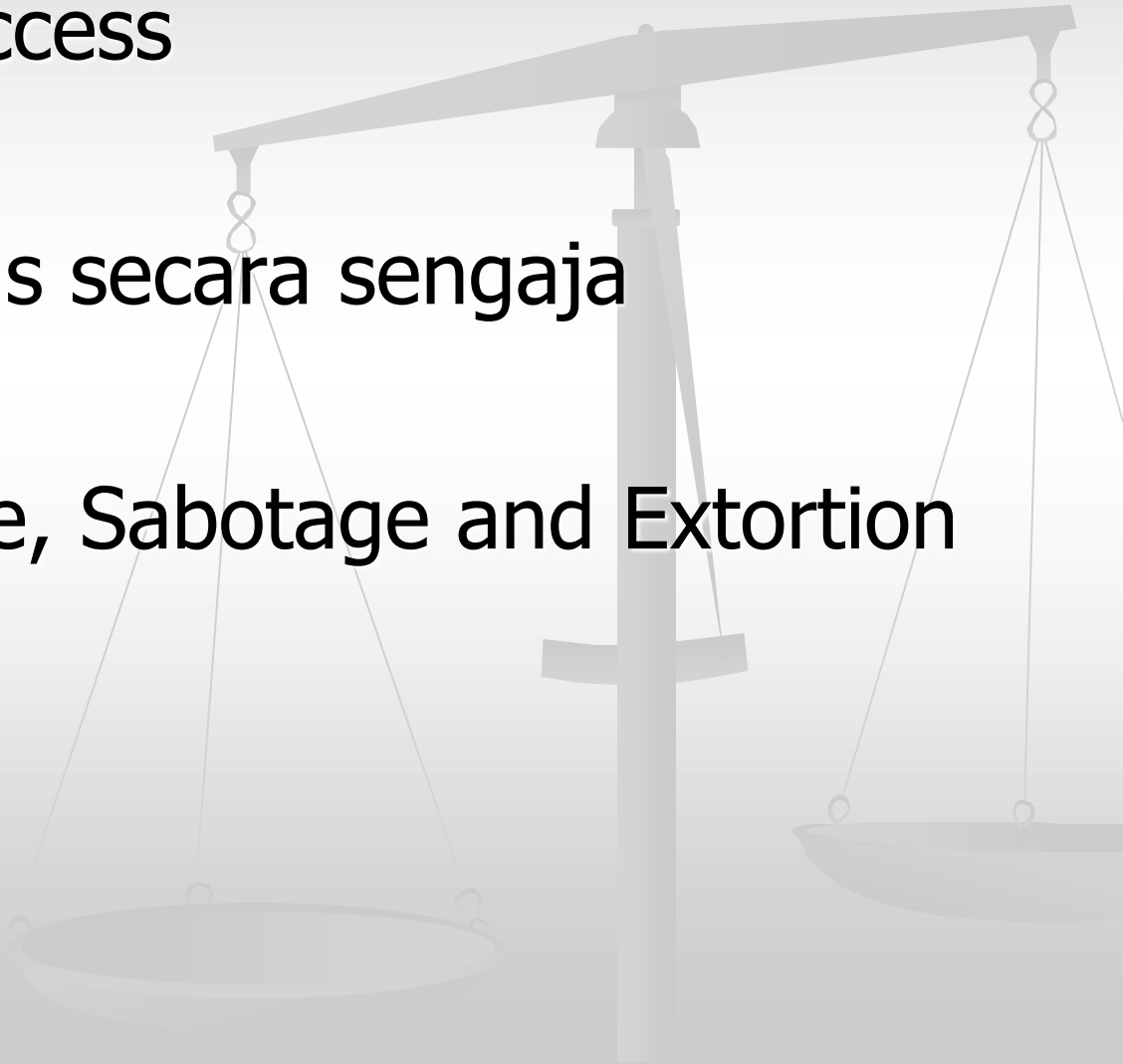
1. Pencurian nomor kartu kredit;
2. Pengambilalihan situs web milik orang lain;
3. Pencurian akses internet yang sering dialami oleh ISP;
4. Kejahatan nama domain;
5. Persaingan bisnis dengan menimbulkan gangguan bagi situs saingannya.

Jenis Cybercrime

- Jenis aktivitas
- Motif kegiatan
- Sasaran Kejahatan

Jenis Cybercrime Berdasarkan Jenis Aktivitas

- Unauthorized Access
- Illegal contents
- Penyebaran virus secara sengaja
- Data Forgery
- Cyber-Espionage, Sabotage and Extortion
- Cyberstalking



Jenis Cybercrime Berdasarkan Jenis Aktivitas

- Carding
- Hacking and Cracking
- Cybersquatting and Typosquatting
- Hijacking
- Cyber Terorism

Jenis Cybercrime Berdasarkan Motif Kegiatan

- Cybercrime sebagai tindakan murni kriminal
- Cybercrime sebagai kejahatan “abu-abu”

Jenis Cybercrime Berdasarakan Sasaran Kejahatan

- Cybercrime yang menyerang individu (Against Person)
- Cybercrime Menyerang Hak Milik (Against Property)
- Cybercrime Menyerang Pemerintah (Against Government)

Penanggulangan Cybercrime

- Mengamankan Sistem
- Penanggulangan Global
- Perlunya CyberLaw
- Perlunya Dukungan Lembaga Khusus

Penanggulangan Cybercrime

- Mengamankan Sistem
- Penanggulangan Global
- Perlunya CyberLaw
- Perlunya Dukungan Lembaga Khusus