Penipuan dan Pengamanan Komputer

The Organization for Economic Cooperation and Development

- Modernisasi hukum pidana nasional yg diselaraskan dgn konvensi internasional terkait kejahatan tsb
- Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
- Meningkatkan pemahaman/keahlian aparatur penegak hukum terkait cybercrime
- Meningkatkan kesadaran warga negara mengenai cybercrime dan perlunya mencegah hal tsb
- Meningkatkan kerjasama antar negara melalui perjanjian ekstradisi dan mutual assistance

Penanggulanagan Global dan Pengamanan Sistem

- Cybercrime adl btk-btk kejahatan yg ditimbulkan oleh pemanfaatan teknologi internet. Aktivitas pokoknya adl penyerangan thdp content, sistem komputer dan sistem komunikasi milik orang lain atau milik umum.
- Seringkali diidentikkan dgn computer crime, yaitu
  - "…any illegal act requiring knowlegde of computer technology for its perpetration, investigation, or prosecution" (US Dept. of Justice)
  - "…any illegal, unethical or unauthorised behaviour relating to the automatic processing and/or the transmission of data" (Organization of European Community Development)
  - "Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal" (Andi Hamzah, 1989)

Karakteristik Cybercrime

Dua jenis kejahatan:

- **Kejahatan kerah biru (Blue Collar Crime)**
  - **Dilakukan scr konvensional**
  - **Mpy stereotip tertentu misalnya pelaku dr kelas sosial bawah, kurang terdidik, berpenghasilan rendah, dll**
- **Kejahatan Kerah Putih (Blue Collar Crime)**
  - **Terbagi mjd 4 jenis:**
    - **Kejahatan korporasi**
    - **Kejahatan birokrat**
    - **Malpraktek**
    - **Kejahatan individu**
  - **Mpy stereotip tertentu misalnya pelaku memiliki penghasilan tinggi, berpendidikan, atau memegang jabatan terhormat dlm masyarakat**

Karakteristik Cybercrime (lanj.)

Cybercrime memiliki karakteristik khusus dlm hal:

- Ruang lingkup kejahatan → bersifat global, pelaku anonymous, aktivitas mungkin blm tersentuh hukum
- Sifat kejahatan → non-violence meski akibatnya lebih buruk drpd kejahatan konvensional
- Pelaku kejahatan → tdk mudah diidentifikasi, lbh bersifat universal
- Modus kejahatan → modus operandinya adl penggunaan teknologi informasi
- Jenis kerugian yg timbul → materiil, non-materiil (waktu, nilai, jasa, harga diri, martabat, kerahasiaan informasi, sosial budaya, politik)

Jenis Cybercrime

Berdasar jenis aktivitasnya:

- Unauthorized Access
- Illegal Content
- Penyebaran virus dengan sengaja
- Data Forgery
- Cyber Espionage, Sabotage and Extortion
- Cyberstalking
- Carding
- Hacking and Cracking
- Cybersquatting and Typosquatting
- Hijacking
- Cyber Terorism

Jenis Cybercrime

- **Unauthorized Access**
  - **Memasuki atau menyusup ke dlm sistem komputer scr tdk sah, tanpa izin/sepengetahuan pemilik**
  - **Misalnya port scanning atau probing (melihat servis apa saja yg ada di server target) menngunakan nmap atau superscan**
  - **Misalnya cyber-tresspass seperti spam email, breaking ke PC, dll**
- **Illegal Content**
  - **Memasukkan data atau informasi ke internet ttg suatu hal yg tdk benar, tdk etis, melanggar hukum, atau mengganggu ketertiban umum**
  - **Misalnya pornografi dll**

Jenis Cybercrime

- **Data Forgery**
  - Bertujuan memalsukan data-data pd dokumen-dokumen penting yg ada di internet
- **Cyber Espionage, Sabotage, and Extortion**
  - Cyber Espionage memanfaatkan jaringan internet utk melakukan kegiatan mata-mata kpd pihak lain dgn cara memasuki sistem jaringan komputer sasaran
  - Sabotage and Extortion mrpk jenis kejahatan yg dilakukan dg membuat gangguan, perusakan, atau penghancuran thdp suatu data, program komputer atau sistem jaringan komputer yg terhubung dgn internet
- **Cyberstalking**
  - Dilakukan utk mengganggu atau melecehkan seseorang dg memanfaatkan komputer

Jenis Cybercrime

- **Carding**
  - **Dilakukan utk mencuri nomor kartu kredit milik orang lain dan digunakan dlm transaksi perdagangan mll internet (e-commerse)**
- **Hacking and Cracking**
  - **Hacker mengacu pd seseorang yg mpy minat besar utk mempelajari sistem komputer scr detail dan bgmn meningkatkan kapabilitasnya → konotasinya netral**
  - **Cracker bisa dianggap sbg hacker yg memanfaatkan kemampuannya utk melakukan hal-hal yg negatif**
  - **Cracking misalnya pembajakan akun orang lain, melumpuhkan sasaran hingga sasaran tdk dpt memberikan pelayanan, dll**
- **Cybersquatting and Typosquatting**
  - **Cybersquatting mrpk kejahatan yg dilakukan dgn mendaftarkan domain nama perusahaan org lain kmd berusaha menjualnya kpd perusahaan tsb**
  - **Typosquatting adl kejahatan dgn membuat domain yg**

Jenis Cybercrime

- Hijacking
  - **Melakukan pembajakan hasil karya orang lain**
  - **Misalnya: software piracy**
- Cyber Terorism
  - **Cybercrime yg sifatnya mengancam pemerintah atau warganegara, termasuk di antaranya cracking ke situs pemerintah atau militer**

Jenis Cybercrime

Berdasar motif kegiatannya:

- **Cybercrime sbg tindakan murni kriminal**
  - **Motifnya murni kriminalitas**
  - **Internet hanya sbg sarana kejahatan**
  - **Misalnya: carding, penyebaran material bajakan, spamming, dll**
- **Cybercrime sbg kejahatan abu-abu**
  - **Sulit ditentukan motifnya (kriminalitas atau bukan)**
  - **Misalnya: Probing**
    Portscanning
    Cybersquatting
    Typosquatting

Jenis Cybercrime

Berdasar sasaran kejahatannya:

- **Menyerang individu (against person)**
  - **Pornografi**
  - **Cyberstalking**
  - **Cyber-Tresspass, misalnya web hacking, PC breaking, probing, port scanning**
- **Menyerang hak milik (against property)**
  - **Carding**
  - **Typosquatting**
  - **Hijacking**
  - **Data forgery**
- **Menyerang pemerintah (against government)**
  - **Cyber terorism**
  - **Cracking ke situs resmi pemerintah**

Penanggulangan Cybercrime

- Mengamankan sistem
  - Bertujuan utk proteksi baik hardware dan software
  - Misalnya menggunakan antivirus, firewall, physical security computer, encrypt login, atau teknologi digital ID
- Penanggulangan global
  - Cybercrime membutuhkan global action dlm penanggulangannya
  - OECD (The Organization for Economic Cooperation and Development) → guidelines utk pembuat kebijakan yg berhubungan dgn computer-related crime
- Perlunya cyberlaw
- Perlunya dukungan lembaga khusus

OECD guidelines utk kebijakan terkait computer-related crime

- Modernisasi hukum pidana nasional yg diselaraskan dgn konvensi internasional terkait kejahatan tsb
- Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional
- Meningkatkan pemahaman/keahlian aparatur penegak hukum terkait cybercrime
- Meningkatkan kesadaran warga negara mengenai cybercrime dan perlunya mencegah hal tsb
- Meningkatkan kerjasama antar negara melalui perjanjian ekstradisi dan mutual assistance treaties terkait cybercrime