# Cyber Crime, Cyber Law & Cyber Ethic

# Cyber Crime

- merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet.
- sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

# Secara konvensional, kejahatan dibagi menjadi:

**a. Kejahatan kerah biru** *(blue collar crime)*

Jenis kejahatan atau tindak kriminal yang dilakukan secara konvensional seperti misalnya perampokan, pencurian, pembunuhan dan lain-lain.

**b. Kejahatan kerah putih** *(white collar crime)*

Terbagi dalam empat kelompok kejahatan,:

1.Kejahatan korporasi,

2.Kejahatan birokrat,

3.Malpraktek,

4.Kejahatan individu.

# Karakteristik unik dari kejahatan di dunia maya antara lain:

a. Ruang lingkup kejahatan
b. Sifat kejahatan
c. Pelaku kejahatan
d. Modus Kejahatan
e. Jenis kerugian yang ditimbulkan

# JENIS-JENIS CYBERCRIME

# A. Berdasarkan jenis aktifitas yang dilakukannya:

*a. Unauthorized Access*

*b. Illegal Contents*

*c.* **Penyebaran virus secara sengaja**

*d. Data Forgery*

*e. Cyber Espionage, Sabotage, and Extortion*

*f. Cyberstalking*

*g. Carding*

*h. Hacking dan Cracker*

*i. Cybersquatting and Typosquatting*

*j. Hijacking*

*k. Cyber Terorism*

# Penjelasan

*a. Unauthorized Access*

Kejahatan yg terjadi ketika seseorang memasuki/menyusup ke dlm suatu sistem jaringan komputer scr tidak sah, tanpa izin, atau tanpa sepengetahuan pemiliknya

Contoh: *Probing* dan *port*

*b. Illegal Contents*

Kejahatan yg dilakukan dgn memasukkan data/informasi ke internet ttg suatu hal yg tidak benar, tidak etis, dan dapat dianggap melanggar hukum/menggangu ketertiban umum, Contoh: penyebaran pornografi.

**c. Penyebaran virus secara sengaja**

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

### *d. Data Forgery*

Kejahatan yg dilakukan dgn tujuan memalsukan data pada dokumen-dokumen penting yg ada di internet.

### *e. Cyber Espionage, Sabotage, and Extortion*

- *Cyber Espionage*: Kejahatan yg memanfaatkan jaringan internet utk melakukan kegiatan mata-mata terhadap pihak lain, dgn memasuki sistem jaringan komputer pihak sasaran.

- *Sabotage and Extortion*: Kejahatan yg dilakukan dgn membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer/sistem jaringan komputer yg terhubung dgn internet.

### *f. Cyberstalking*

Mengganggu/melecehkan seseorang dgn memanfaatkan komputer, mis. menggunakan e-mail dan dilakukan berulang-ulang.

Kejahatan ini menyerupai teror yg ditujukan kpd seseorang dgn memanfaatkan media internet.

*g. Carding*

Kejahatan yg dilakukan utk mencuri nomor kartu kredit milik orang lain dan digunakan dlm transaksi perdagangan di internet.

*h. Hacking dan Cracker*

*Hacker:* biasanya mengacu pd seseorang yg punya minat besar utk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya.

*Cracker :* orang yg sering melakukan aksi-aksi perusakan di internet.

Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif spt: pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, pelumpuhan target sasaran/DoS

DoS attack (Denial Of Service) yaitu serangan yg bertujuan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan.

### *i. Cybersquatting and Typosquatting*

***Cybersquatting:*** Kejahatan yg dilakukan dgn mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dgn harga yg lebih mahal.

***Typosquatting:*** Kejahatan dgn membuat domain plesetan (mirip dgn nama domain orang lain). Nama tersebut merupakan nama domain saingan perusahaan.

### *j. Hijacking*

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

### *k. Cyber Terorism*

Termasuk cyber terorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah/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.

# B. Berdasarkan Motif Kegiatan

**a. Cybercrime sebagai tindakan murni kriminal**

- Kejahatan yang dilakukan karena motif kriminalitas.
- Menggunakan internet hanya sbg sarana kejahatan.
- Contoh:
  - *Carding*
  - *Webserver,*
  - *Mailing list*
  - *Spamming promosi*

**b. Cybercrime sebagai kejahatan ”abu-abu”**

•Sulit untuk menentukan apakah itu merupakan tindak kriminal atau bukan, krn terkadang motif kegiatannya bukan untuk kejahatan.

•Contoh:

*Probing atau portscanning*.

Sebutan untuk semacam tindakan pengintaian thd sistem milik orang lain dgn mengumpulkan informasi sebanyak-banyaknya dari sistem yg diintai, termasuk sistem operasi yg digunakan, port-port yg ada, baik yg terbuka maupun tertutup.

# C. Berdasarkan Sasaran Kejahatan

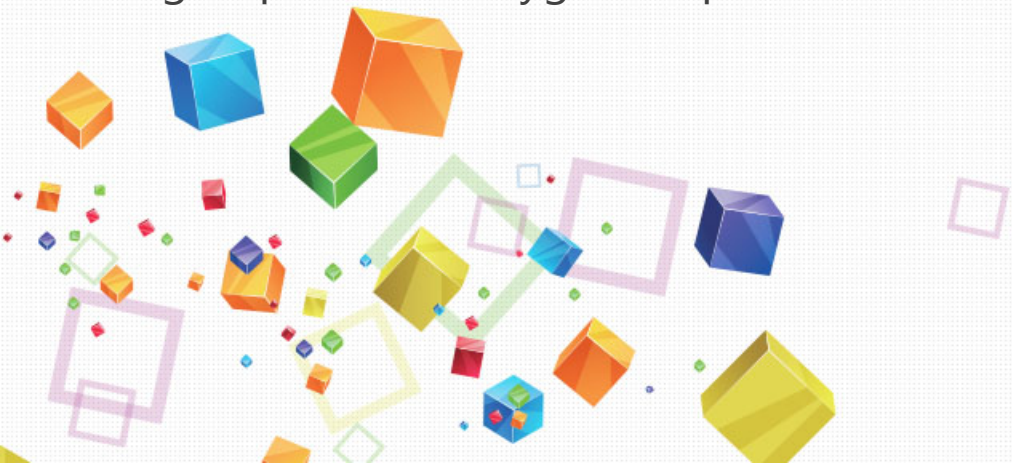
**a. Cybercrime yang menyerang individu (Against Person)**

Kejahatan yg sasarannya ditujukan kpd perorangan/individu yg memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut.

Contoh kejahatan ini antara lain :

- **Pornografi**

Dilakukan dgn membuat, memasang, mendistribusikan, dan menyebarkan material yg berbau pornografi, cabul, serta mengekspos hal-hal yg tidak pantas.



- *Cyberstalking*

Dilakukan utk mengganggu/melecehkan seseorang dgn 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*

Dilakukan melanggar area privasi orang lain seperti misalnya *Web Hacking. Breaking ke PC, Probing, Port Scanning,* dsb.

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

Dilakukan utk menggangu/menyerang hak milik orang lain.

Contoh:

- pengaksesan komputer secara tidak sah melalui dunia cyber,
- pemilikan informasi elektronik scr tidak sah/pencurian informasi,
- carding,
- cybersquating,
- hijacking,
- data forgery

**c. Cybercrime menyerang pemerintah (Againts Government)**

Dilakukan dgn tujuan khusus yaitu penyerangan thd pemerintah.

Contoh:

**C*yber terorism*** sbg tindakan yg mengancam pemerintah termasuk juga cracking ke situs resmi pemerintah/situs militer.

# Penanggulangan Cybercrime

- Aktivitas pokok dari cybercrime adalah penyerangan thd content, computer system dan communication system milik orang lain atau umum di dalam cyberspace.
- Cybercrime dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan.
- Berikut ini cara penanggulangan cybercrime :

**a. Mengamankan sistem**

- Tujuan sebuah sistem keamanan adalah mencegah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yg tidak diinginkan.
- Membangun sebuah keamanan sistem hrs merupakan langkah-langkah yg terintegrasi pd keseluruhan subsistemnya, dgn tujuan dapat mempersempit atau bahkan menutup adanya celah-celah *unauthorized actions* yg merugikan.
- Pengamanan secara personal dpt 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.

**b. Penanggulangan Global**

•Th.1986 The Organization for Economic Cooperation and Development (OECD) telah membuat guidelines bagi para pembuat kebijakan yg berhubungan dgn computer-related crime, dgn memublikasikan laporannya berjudul Computer-Related Crime : *Analysis of Legal Policy*.

•Menurut OECD, beberapa langkah penting yg hrs dilakukan setiap negara dlm penanggulangan cybercrime adalah :

a.melakukan modernisasi hukum pidana nasional beserta hukum acaranya.

b.meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.

c.meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime.

d.meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.

e.meningkatkan kerjasama antarnegara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime.

# Cyberlaw

- Perkembangan teknologi yg sangat pesat, membutuhkan pengaturan hukum yg berkaitan dgn pemanfaatan teknologi tersebut.
- Permasalahan yg sering muncul adalah bagaimana menjaring berbagai kejahatan komputer dikaitkan dgn ketentuan pidana yg berlaku karena ketentuan pidana yg mengatur tentang kejahatan komputer yg berlaku saat ini masih belum lengkap
- Banyak kasus yang membuktikan bahwa perangkat hukum di bidang TI masih lemah.

# Perlunya Dukungan Lembaga Khusus

- Lembaga-lembaga khusus, baik milik pemerintah maupun NGO (Non Government Organization), diperlukan sbg upaya penanggulangan kejahatan di internet.

- AS memiliki *Computer Crime and Intellectual Property Section* (CCIPS) sbg sebuah divisi khusus dari U.S. Departement of Justice. Institusi ini memberikan informasi ttg cybercrime, melakukan sosialisasi secara intensif kpd masyarakat, serta melakukan riset-riset khusus dlm 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.

# Cyber Ethic

- Terjadinya pergeseran nilai sosial masyarakat menjadi sangat tinggi ketika komputer telah menjadi gaya hidup yg tidak bisa terelakkan bagi masyarakat modern
- Dibanjiri dengan '**warga negara**' baru yg tidak terpisahkan oleh ruang & waktu
- Rentan dgn atmosfer kejahatan
- Konvensi-konvensi, etika, dan hukum hrs dibuat demi menjaga eksistensi dunia maya

# Karakteristik dunia maya/cyber space

- Beroperasi secara virtual
  - tdk hrs bertemu fisik
  - selain manusia penghuninya adalah data, informasi, email, ide, ilmu pengetahuan , dll
- Selalu berubah dgn cepat

  - ada kemudahan akses data, update data,
- Tdk mengenal batas teritorial

  tdk terbatas ruang dan waktu, pelanggaran semakin kompleks dan sulit ditangani
- *Anonymouse*

  - Penghuni tanpa harus dgn identitas asli
- Informasinya bersifat publik

# Beberapa alasan pentingnya etika dalam dunia maya:

- Pengguna internet berasal dari berbagai negara yang mungkin memiliki budaya, bahasa dan adat istiadat yang berbeda-beda.
- Pengguna internet → *anonymouse,* tidak mengharuskan ID asli dalam berinteraksi.
- Berbagai macam fasilitas yang diberikan dalam internet memungkinkan seseorang untuk bertindak etis seperti misalnya ada juga penghuni yang suka iseng dengan melakukan hal-hal yang tidak seharusnya dilakukan.
- Harus diperhatikan bahwa pengguna internet akan selalu bertambah setiap saat dan memungkinkan masuknya "penghuni" baru didunia maya tersebut.

# Netiquette

- Merupakan Etika dalam menggunakan Internet.  Internet sebagai sebuah kumpulan komunitas,
- Perlu aturan yang akan menjadi acuan orang-orang sebagai pengguna Internet.
- Aturan yg menyangkut batasan dan cara yang terbaik dalam memanfaatkan fasilitas Internet.
- bermanfaat dan membantu Anda dalam berkomunikasi dan berinteraksi dengan orang lain tanpa harus mengalami masalah atau tanpa harus mengalami salah pengertian dengan orang lain.
- Netiquette memiliki fungsi  = etiket yang ada di dalam lingkungan sosial manusia, yaitu merupakan tata krama atau sopan santun yang harus diperhatikan dalam pergaulan agar hubungan selalu baik.

# CONTOH ETIKA BERINTERNET:

**Pengguna tidak diperbolehkan:**

•Terlibat dlm penyalahgunaan email, atau spam, termasuk (tidak terbatas pada) memposkan atau mempos-silang artikel yg tdk diinginkan dgn pesan yg sama/bersubstansi sama kpd penerima yg tidak meminta utk menerima pesan tsb.

•Terlibat dlm kegiatan yg ditujukan utk membujuk, meminta, atau sebaliknya merekrut pengguna-pengguna dari situs utk bergabung dgn organisasi kecuali kegiatan tersebut dinyatakan secara jelas telah mendapatkan ijin/otorisasi secara tertulis, oleh suatu perusahaan dan diizinkan oleh undang-undang RI dan jika Anda mengakses situs dari negara lain, oleh undang-undang yg berlaku di negara Anda;

- Bertindak yg bertujuan utk menipu/menyesatkan orang, berupaya meniru atau menggantikan afiliasi ke orang pribadi manapun atau memalsukan tajuk atau sebaliknya memanipulasi identifikasi guna menyamarkan aslinya atas segala yg diposkan dan atau dikirim atau ditransmisikan melalui produk dan/atau layanan;

- Meniru orang pribadi lain atau menggunakan nama tanpa seizin guna membuat identitas palsu dan/atau alamat surat elektronik palsu atau untuk menggantikan identitas orang yang asli untuk melakukan segala bentuk komunikasi ke situs dan/atau pemiliknya;

- Mengubah, mengakses, atau membuat data yang tersimpan pada komputer dapat diakses, yang telah diakses melalui situs;

- Membuat, menyediakan atau mengunggah berkas yang berisi perangkat lunak atau materi lain yang tidak dimiliki sendiri oleh Anda atau tidak dilisensikan kepada Anda dengan cara yang benar;

- Menggunakan produk dan/atau layanan atau situs untuk memposkan atau mentransmisikan, melalui pencatatan dan atau pendaftaran, melalui ulasan, melalui
komentar, melalui saran, melalui ide, melalui pertanyaan, atau sebaliknya, apa pun yang termasuk dalam tindakan melanggar hukum, mengandung fitnah, diskriminatif, porno, menyinggung, vulgar, bersifat mengancam, kasar, mengandung pelecehan, berbahaya, penuh kebencian, tidak sopan, menjurus seksual, atau mengandung pornografi anak, penghinaan agama atau ras, mengandung keberatan berdasarkan etnis dan ras atau sebaliknya dengan cara apa pun mengancam atau atau mendorong kekerasan pada tubuh atau sejenisnya atau yang dapat melanggar hak pribadi orang;

- Menggunakan produk dan/atau layanan utk memberikan penawaran yg bertujuan utk menipu, utk menjual atau membeli produk, item, atau layanan atau utk melakukan penawaran atau melakukan permintaan utk segala jenis/ bentuk penipuan keuangan jenis apa pun seperti “skema piramida” dan “surat berantai”;

- Menggunakan produk dan/atau layanan dgn cara apapun yg dpt melanggar hak kekayaan intelektual (mis. hak cipta atau merek dagang) atau hak kekayaan lainnya, termasuk (tidak terbatas pada) pengalihan dari perangkat lunak bajakan;

- Menggunakan produk dan/atau layanan dgn cara apapun yg dpt merusak, mengganggu, memforsir, atau membuat produk dan/atau layanan tidak berfungsi atau mengganggu penggunaan atau kenikmatan menggunakan dari pihak lain terhadap produk dan/atau layanan tersebut;

спасибо 谢谢
GRACIAS
THANK YOU
ありがとうございました MERCI
DANKE धन्यवाद
شُكراً OBRIGADO