



**SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI**

ETIKA PROFESI

Krisna Panji, S.Kom. M.M | panji@nurulfikri.ac.id | 0857-1414-1089

TEKNIK INFORMATIKA | SISTEM INFORMASI



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

PERTEMUAN KE 14

CYBERCRIME : PENCEGAHAN & PENANGGULANGANNYA



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Jenis Kejahatan Konvensional :

a) Kejahatan kerah biru (blue collar crime)

Kejahatan yang dilakukan secara konvensional seperti perampokan, pencurian, pembunuhan dll. Pelaku digambarkan memiliki stereotip tertentu, misal : dari kelas sosial bawah, kurang terdidik, berpenghasilan rendah.

b) Kejahatan kerah putih (white collar crime)

Kejahatan ini terbagi dalam 4 (empat) kelompok :

a) Kejahatan korporasi

b) Kejahatan birokrat

c) Malpraktek

d) Kejahatan individu

Pelakunya memiliki penghasilan tinggi, berpendidikan, memegang jabatan-jabatan terhormat di masyarakat



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Cybercrime sendiri merupakan kejahatan yang muncul akibat adanya komunitas dunia maya di internet.

Karakteristik unik dari cybercrime menyangkut 5(lima) hal yaitu :

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



Jenis Cybercrime

1. Berdasarkan Jenis Aktivitasnya
2. Berdasarkan Motif Kegiatannya
3. Berdasarkan Sasaran Kejahatannya



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

1. Berdasarkan Jenis Aktivitasnya

- a. Illegal Contents
- b. Penyebaran Virus secara sengaja
- c. Data Forgery (pemalsuan data)
- d. Cyber Espionage, Sabotage and Extortion (kegiatan mata-mata dengan memasukan sistem jaringan komputer, membuat gangguan kerusakan dan penghancuran suatu data program komputer)
- e. Cyberstalking
- f. CardingHacking dan Cracking
- g. Cybersquatting and Typosquatting (mendaftarkan nama domain dengan niat buruk untuk mengambil keuntungan, kejahatan dengan membuat doamin plesetan yaitu domain yang mirip dengan domain orang lain)
- h. Hijacking (kegiatan yang berusaha menyusup ke sisitem melalui sistem operasional yang dijalankan oleh hacker)
- i. Cyber Terrorism



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

2. Berdasarkan Motif Kegiatannya
 - a. Cybercrime sebagai tindakan murni kriminal
 - b. Cybercrime sebagai kejahatan “abu-abu”



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

3. Berdasarkan Sasaran Kejahatan

Dibagi dalam 3 kategori :

1. Cybercrime yang menyerang individu (*Against Person*) : pornografi, cyberstalking, cyber-trespass
2. Cybercrime Menyerang Hak Milik (*Againts Property*)
3. Cybercrime Menyerah Pemerintah (*Againts Government*)



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Bentuk-bentuk Cybercrime :

- 1). Kejahatan Dunia Maya yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer.
 - a). Illegal access (akses secara tidak sah terhadap sistem komputer).
 - b). Data interference (mengganggu data komputer).
 - c). System interference (mengganggu sistem komputer).
 - d). Illegal interception in the computers, systems and computer networks operation (intersepsi secara tidak sah terhadap komputer, sistem, dan jaringan operasional komputer).
 - e). Data Theft (mencuri data).
 - f). Data leakage and espionage (membocorkan data dan memata-matai).
 - g). Miss use of devices (menyalahgunakan peralatan komputer).



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

2). Kejahatan Dunia Maya yang menggunakan komputer sebagai alat kejahatan

- a. Credit card fraud (penipuan kartu kredit).
- b. Bank fraud (penipuan terhadap bank)
- c. Service Offered fraud (penipuan melalui penawaran suatu jasa)
- d. Identity Theft and Fraud (pencurian identitas dan penipuan)
- e. Computer-related fraud (penipuan melalui komputer)
- f. Computer-related forgery (pemalsuan melalui komputer)
- g. Computer-related betting (perjudian melalui komputer)
- h. Computer-related Extortion and Threats (pemerasan dan pengancaman melalui komputer).



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

3). Kejahatan Dunia Maya yang berkaitan dengan isi atau muatan data atau sistem Komputer.

- a) Child pornography (pornografi anak).
- b) Infringements Of Copyright and Related Rights (pelanggaran terhadap hak cipta dan hak-hak terkait).
- c) Drug Traffickers (peredaran narkoba).



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

PENCEGAHAN

- **Gunakan Security Software yang Up to Date**

Penting untuk menjaga Security Software kita tetap terbaru atau up to date. Perlakuan ini akan memberikan pendefinisian kembali atas ancaman cybercrime maupun virus yang belum didefinisikan pada versi sebelumnya. Pembaruan ini sangat berguna bagi pengguna yang cukup sering menggunakan koneksi internet. Disarankan bagi para pemilik gadget menggunakan *Security Software* untuk membuka akses ke internet. Hal ini harus dilakukan minimal dua atau tiga kali dalam seminggu. Saat pengguna online, secara otomatis Security Software akan meng-up to date versi terbarunya.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- **Melindungi Komputer**

Menjaga keamanan, paling tidak kita harus mengaplikasikan tiga program, yaitu

1. **Antivirus** : menjaga perangkat komputer dari virus
2. **Antispyware** : melindungi data pemakai agar tidak ada yang melacak kebiasaan kita saat online
3. **Firewall** : sistem atau perangkat yang memungkinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- **Buat Password yang sangat sulit**

Bagaimana dengan password akun-akun kita seperti , akun jejaring sosial atau akun tabungan online kita? sudah kah menggunakan password yang susah di tebak? Jika belum cepat ganti password akun-akun kita untuk mencegah terjadinya cybercrime terhadap kita. Bila bisa masukan campuran huruf kecil, besar dan angka pada setiap akun kita agar memperkuat kata sandi kita. Contoh kata sandi dengan di campur dengan angka **C0ntOhNy4** . Kata sandi ini cukup kuat untuk sandi akun kita karenana di campur dengan huruf kecil, besar dan angka.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- **Back up data**

Sebaiknya para pengguna komputer memiliki salinan dari dokumen pribadinya, entah itu berupa foto, musik, atau yang lainnya. Ini bertujuan agar data kita masih tetap bisa terselamatkan bila sewaktu-waktu terjadi pencurian data atau ada kesalahan pada sistim komputer kita.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- Jangan Sembarangan Mengklik Link yang Muncul di Social Network

Entah melalui Facebook, Twitter, atau Blog, sering kita temui link yang menarik perhatian. Walaupun tidak mengetahui jelas soal apa link tersebut, sajian yang menarik berupa iklan atau sekedar kuesioner dan angket membuat kita membukanya. Tidak sedikit hal ini dijadikan peluang cybercrime atau penyebaran virus komputer. Tidak jarang pula link seperti ini dikirimkan oleh teman atau saudara kita sendiri. Maka dari itu, lebih baik hanya membuka iklan yang kita butuhkan saja. Jangan tergiur akan sesuatu yang malah akan membuat kita terjebak dalam cybercrime atau virus komputer



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- **Ganti Password Secara Berkala**

Melihat banyak dan mudahnya cybercrime dilakukan—sampai 15 kasus perdetik, tidak menutup kemungkinan password terpanjang pun dapat dibajak apabila digunakan bertahun-tahun. Maka, disarankan untuk mengganti password tersebut, baik secara berkala atau acak.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

PENANGGULANGAN

- Pengamanan Sistem

- ✓ Tujuan yang paling nyata dari suatu sistem keamanan adalah meminimasi dan mencegah adanya kerusakan bagian dalam sistem, karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem ini harus terintegrasi pada keseluruhan subsistem untuk mempersempit atau bahkan menutup adanya celah-celah unauthorized actions yang merugikan.
- ✓ Pengamanan secara personal dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya tahap pengamanan fisik dan pengamanan data. Pengamanan sistem melalui jaringan dapat juga dilakukan dengan melakukan pengamanan terhadap FTP, SMTP, Telnet. dan Pengamanan Web Server.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

• **Penanggulangan Global**

OECD (The Organization for Economic Cooperation and Development) telah merekomendasikan beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan Cybercrime, yaitu :

- Melakukan modernisasi hukum pidana nasional dengan hukum acaranya, yang diselaraskan dengan konvensi internasional.
- Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
- Meningkatkan pemahaman serta keahlian aparaturnya mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan cybercrime.
- Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.
- Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- **Perlunya Cyberlaw**

- Cyberlaw merupakan istilah hukum yang terkait dengan pemanfaatan TI. Istilah lain adalah hukum TI (Law of IT), Hukum Dunia Maya (Virtual World Law) dan hukum Mayantara. Perkembangan teknologi yang sangat pesat membutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut. Hanya saja, hingga saat ini banyak negara yang belum memiliki perundang-undangan khusus di bidang teknologi informasi, baik dalam aspek pidana maupun perdata-nya.
- Kekhawatiran akan kejahatan mayantara di dunia sebetulnya sudah dibahas secara khusus dalam suatu lokakarya (“Workshop On Crimes To Computer Networks”) yang diorganisir oleh UNAFEI selama kongres PBB X/2000 berlangsung.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

- Dengan Kesimpulan :

CRC (computer-related crime) harus dikriminalisasikan. Diperlukan hukum acara yang tepat untuk melakukan penyidikan dan penuntutan terhadap penjahat cyber. Harus ada kerjasama pemerintah dan industri terhadap tujuan umum pencegahan dan penanggulangan kejahatan komputer agar internet menjadi tempat yang aman. Diperlukan kerja sama internasional untuk menelusuri para penjahat di internet. PBB harus mengambil langkah / tindak lanjut yang berhubungan dengan bantuan dan kerjasama teknis dalam penganggulangan CRC.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Ruang lingkup dari *cyberlaw*

- Hak cipta, hak merek, pencemaran nama baik (defamation), *hate speech* (fitnah, penistaan dan penginaan)
- Serangan terhadap fasilitas komputer (*hacking, viruses, ilegal access*), pengaturan sumber daya internet (*IP addresses, domain name*),
- Kenyamanan individu (privacy), tindakan kriminal yang biasa menggunakan TI sebagai alat,
- Isu prosedural (yurisdiksi, pembuktian, penyidikan), transaksi elektronik dan digital, pornografi,
- Perlindungan konsumen, pemanfaatan internet dalam aktifitas keseharian (*e-commerce, e-government, e-education, e-medics*).



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Perlunya Dukungan Lembaga Khusus

- Lembaga khusus yang dimaksud adalah milik pemerintah dan NGO (Non Government Organization) diperlukan sebagai upaya penanggulangan kejahatan di internet. Lembaga ini diperlukan untuk memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime. Indonesia sendiri sudah memiliki IDCERT (Indonesia Computer Emergency Response Team) yang diperlukan bagi orang-orang untuk melaporkan masalah-masalah keamanan komputer.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Strategi Penanggulangan Cybercrime di Indonesia

a. Strategi Jangka Pendek

- 1) Penegakan hukum pidana: salah satu manifestasi untuk membuat hukum tidak hanya sebagai barang hukum tidak hanya sebagai barang rongsokan yang tidak berguna.
- 2) Mengoptimalkan UU khusus lainnya. Sektor cyber space banyak bersentuhan dengan sektor - sektor lain yang telah memiliki aturan khusus dalam pelaksanaannya. Ada beberapa aturan yang bersentuhan dengan dunia cyber yang dapat digunakan untuk menjerat pelaku cybercrime, sehingga sepek terjangnya semakin sempit.
- 3) Rekrutment aparat penegak hukum. Diutamakan dari masyarakat yang menguasai dunia komputer dan internet di samping kemampuan lain yang dipersyaratkan.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Strategi Penanggulangan Cybercrime di Indonesia

b. Strategi Jangka Menengah

1. *Cyber police* : orang-orang khusus yang dilatih dan dididik untuk melakukan penyidikan cybercrime. Pola pembentukannya merupakan bagian dari upaya reformasi kepolisian.
2. Kerjasama internasional. Hal ini dikarenakan kejahatan modern sudah melintasi batas-batas negara yang dilakukan berkat dukungan teknologi, sistem komunikasi, dan transportasi. Hal ini dapat menunjukkan adanya sistem kepolisian yang terbuka, dan mendapatkan keuntungan dalam kerjasama mengatasi penjahat-penjahat internasional yang masuk melintasi wilayah hukum Indonesia



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

Strategi Penanggulangan Cybercrime di Indonesia

Strategi Jangka Panjang

1. Membuat UU *cybercrime*. Tujuannya adalah untuk pemberatan atas tindakan pelaku agar dapat menimbulkan efek jera dan mengatur sifat khusus dari sistem pembuktian.
2. Membuat perjanjian bilateral. Media internet adalah media global, yang tidak memiliki batasan waktu dan tempat. *Cybercrime* dapat melibatkan beberapa negara, sehingga perlu hubungan di jalur bilateral untuk menaggulangnya.



SEKOLAH TINGGI TEKNOLOGI TERPADU NURUL FIKRI

TERIMA KASIH