Materi Online 3

MATA KULIAH ISU SOSIAL DAN KEPROFESIAN TEKNOLOGI INFORMASI

KODE MATA KULIAH CCS210

DISUSUN OLEH
NIZIRWAN ANWAR & TEAM

FAKULTAS ILMU KOMPUTER
UNIVERSITAS ESA UNGGUL
JAKARTA
2018

MATERI

COMPUTER AND INTERNET CRIME

Computer and Internet Crime

Nizirwan Anwar

Pendahuluan (1)

- Dalam sebuah situs informasi www.wikipedia.org kejahatan dunia maya (Inggris: cybercrime) adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain adalah penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas, pornografi anak, dll.

Pendahuluan (2)

- Cybercrime sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal. Kejahatan Komputer adalah segala aktifitas tidak sah yang memanfaatkan komputer untuk tidak pidana . Sekecil apapun dampak atau akibat yang ditimbulkan dari penggunaan komputer secara tidak sah atau ilegal merupakan suatu kejahatan.

Pendahuluan (3)

- Secara umum dapat disimpulkan sebagai perbuatan atau tindakan yang dilakukan dengan menggunakan komputer sebagai alat/sarana untuk melakukan tidak pidana atau komputer itu sendiri sebagai objek tindak pidana. Dan dalam arti sempit kejahatan komputer adalah suatu perbuatan melawan hukum yang dilakukan dengan teknologi komputer yang canggih.

Apakah Cybercrime … ???

- Salah satu definisi Cyber crime, computer crime, adalah perbuatan melawan hukum yang dilakukan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Mengapa terjadi CC … ???

- Internet sebagai hasil rekayasa teknologi bukan hanya menggunakan kecanggihan teknologi komputer tapi juga melibatkan teknologi telekomunikasi di dalam pengoperasiannya.
- Pada perkembangannya, ternyata penggunaan internet tersebut membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti-sosial dan perilaku kejahatan yang selama ini dianggap tidak mungkin terjadi.
- Sebagaimana sebuah teori mengatakan: "crime is a product of society its self", yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang melahirkan suatu kejahatan.
- Semakin tinggi tingkat intelektualitas suatu masyarakat, semakin canggih pula kejahatan yang mungkin terjadi dalam masyarakat itu.

Hacker vs Cracker …!!!

- **Hacker** adalah sebutan untuk mereka yang memberikan sumbangan yang bermanfaat kepada jaringan komputer, membuat program kecil dan membagikannya dengan orang-orang di Internet.
- Mencari, mempelajari dan mengubah sesuatu untuk keperluan hobi dan pengembangan dengan mengikuti legalitas yang telah ditentukan oleh developer game.
- Para hacker biasanya melakukan penyusupan-penyusupan dengan maksud memuaskan pengetahuan dan teknik. Rata - rata perusahaan yang bergerak di dunia jaringan global (internet) juga memiliki hacker.

Hacker vs Cracker …!!!

- **Cracker** adalah sebutan untuk mereka yang masuk ke sistem orang lain dan cracker lebih bersifat destruktif, biasanya di jaringan komputer, mem-bypass password atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-deface (merubah halaman muka web) milik orang lain bahkan hingga men-delete data orang lain, mencuri data.

- Pada umumnya melakukan cracking untuk keuntungan sendiri, maksud jahat, atau karena sebab lainnya karena ada tantangan

Level Hacker … #fyi

- Elite
- Semi Elite
- Developed Kiddie
- Script Kiddie
- Lamer

Kategori Cyber Crime

- **Eoghan Casey** mengkategorikan *cybercrime* dalam 4 kategori yaitu:
  1) *A computer can be the object of Crime.*
  2) *A computer can be a subject of crime.*
  3) *The computer can be used as the tool for conducting or planning a crime.*
  4) *The symbol of the computer itself can be used to intimidate or deceive.*

Bentuk CC (1)

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi ini dalam beberapa literatur dan prakteknya dikelompokan dalam beberapa bentuk, antara lain:

- **Unauthorized Access to Computer System and Service** yaitu Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.
- **Illegal Contents** yaitu Merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

Bentuk CC (2)

- **Data Forgery**

  Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

- **Cyber Espionage**

  Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*.

Bentuk CC (3)

- **Cyber Sabotage and Extortion**

  Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

- **Offense against Intellectual Property**

  Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet.

- **Infringements of Privacy**

  Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia

Modus Operand Cyber Crime

- Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi ini dikelompokkan dalam beberapa bentuk sesuai modus operandi yang ada, antara lain:
  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. *Infringements of Privacy*

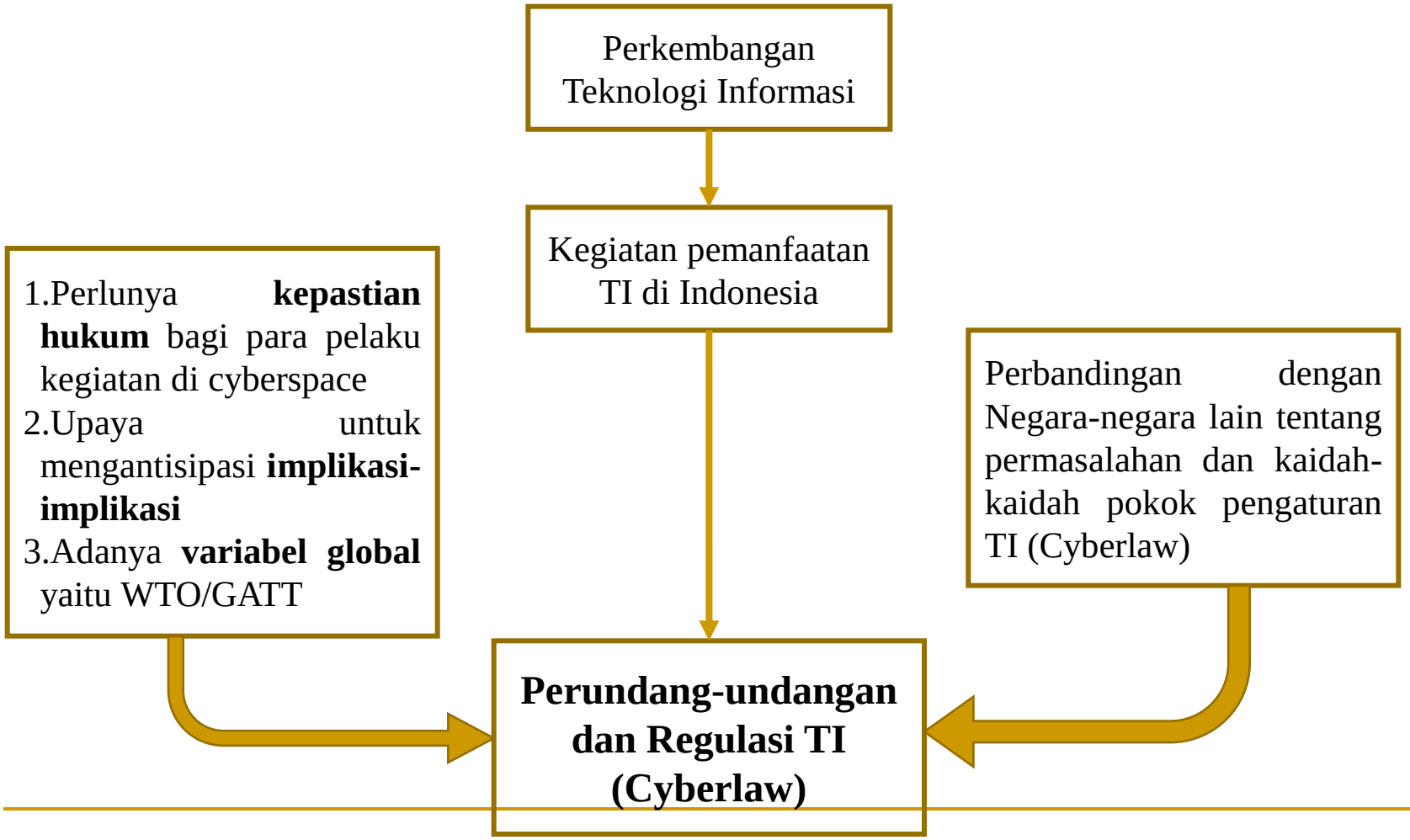
Kiat dalam pencegahan kejahatan CC

- Beberapa kiat yang dapat digunakan dan dicoba untuk meminimalisir CC, antara lain ;
  1) Melindungi Komputer
  2) Melindungi Identitas
  3) Selalu Up to Date
  4) Amankan E-mail
  5) Melindungi Account
  6) Membuat Salinan
  7) Cari Informasi

Perangkat pengamanan

1. Internet Firewall
2. Kriptografi
3. Secure Socket Layer (SSL)

Urgensi pengaturan teknologi informasi (cyberlaw)



Kasus CC

- **Wajah Kasus di Indonesia (1)**

  Indonesia pernah menempati urutan ke 2 setelah Negara Ukraina asal pelaku kejahatan carding (pembobolan kartu kredit). Dari 124 kasus pembobolan kartu kredit lewat internet yang dilakukan hacker di Asia-Pacific, 123 di antaranya dilakukan para tersangka dari berbagai kota di Indonesia. Sebagian besarnya ditengarai berasal dari Yogyakarta, Jakarta, Malang dan Medan. Korbannya sendiri didominasi oleh mereka yang berdomisili di AS, sebanyak 88 orang. Bahkan, data tahun lalu menunjukkan adanya tindakan yang digolongkan sebagai tindak terorisme dengan mengacak sistem informasi jaringan sebuah institusi di AS oleh hacker asal Bandung dengan menggunakan e-mail atau surat elektronik via internet.

Kasus CC

- **Wajah Kasus di Indonesia (2)**

  Money Laundering erat kaitannya dengan kegiatan mentransfer dana. Kegiatan transfer dana itu sendiri saat ini banyak dilakukan dengan menggunakan teknologi, semacam wire transfer, ATM, dan masih banyak lagi. Bahkan saat ini metode transfer dana yang banyak digunakan karena sangat cepat adalah dengan menggunakan RTGS (Real Time Gross Settlement).

Kasus CC

- **Wajah Kasus di Indonesia (3)**

  Ketika krisis di Timor-Timur sempat terjadi peperangan antara hacker indonesia dan australia. Serta ketika hubungan Indonesia dan Malaysia yang memanas karena masalah perbatasan. Beberapa situs pemerintah Malaysia sempat didevace oleh Hakcer Indonesia, dan dari Malayasia juga membalas dengan mendevace situs pemerintah daerah di Indonesia.

Kasus CC

- **Wajah Kasus di Indonesia (4)**

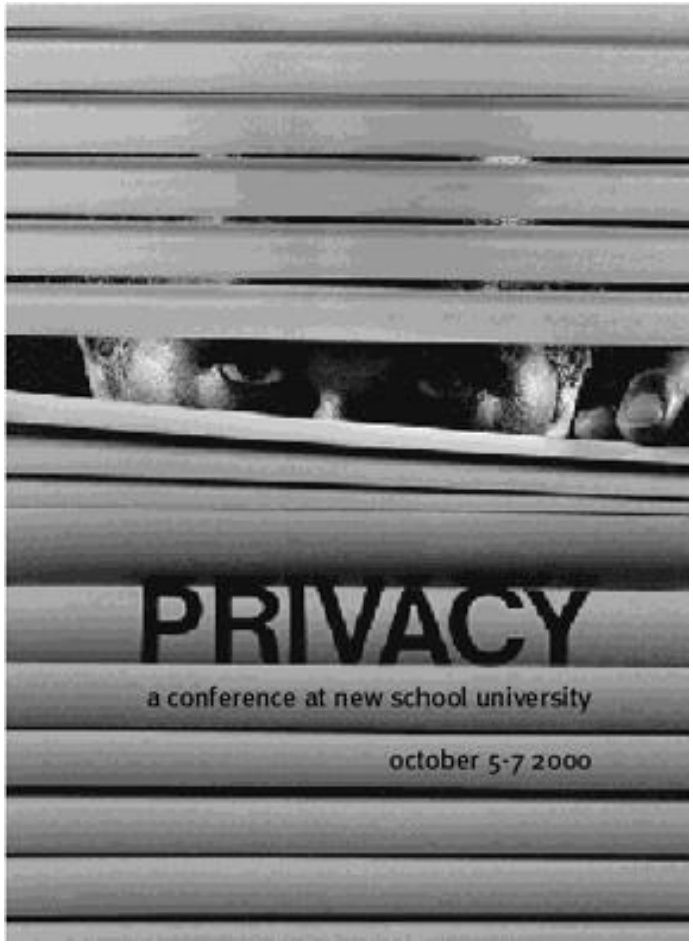
  Dani Firmansyah, konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta berhasil membobol situs milik Komisi Pemilihan Umum (KPU) di http://tnp.kpu.go.id dan mengubah nama-nama partai di dalamnya menjadi nama-nama "unik", seperti Partai Kolor Ijo, Partai Mbah Jambon, Partai Jambu, dan lain sebagainya. Dani menggunakan teknik SQL Injection(pada dasarnya teknik tersebut adalah dengan cara mengetikkan string atau perintah tertentu di address bar browser) untuk menjebol situs KPU. Kemudian Dani tertangkap pada hari Kamis, 22 April 2004.

4 (empat) Isu Etika Era Informasi

- Privacy
- Accuracy
- Property
- Accessibility

Privacy

- Informasi seseorang atau terkait seseorang mana yang:
- Boleh dibuka kepada orang lain?
- Dalam kondisi/syarat apa?
- Apa yang dapat seseorang sembunyikan dari orang lain?



Accuracy

- Siapa yang bertanggung-jawab kepada:
- Autentikasi, ketepatan, dan keakuratan informasi?
- Siapa yang harus menanggung bila ada error di informasi dan bagaimana kesalahan itu berakibat kepada sistem secara keseluruhan?

Property

- Siapa pemilik informasi? Bagaimana harganya? Siapa channel atau bagaimana informasi itu mengalir? Siapa yang boleh mengakses?

Accessibility

- Informasi apa yang dapat diperoleh oleh seseorang atau organisasi? Dalam kondisi seperti apa?
- Sama dengan “Privacy” tapi dari sudut pandang pengguna informasi.