

# Cyber Crime : Modus, Penyebab dan Penanggulangannya

Arif Basofi  
@PENS 2014

# Referensi

- Teguh Wahyono, Etika Komputer dan Tanggung Jawab Profesional di Bidang Teknologi Informasi, Penerbit Andi Yogyakarta, 2006.
- Arief Wibowo, Universitas Budi Luhur, 2008.
- ...

# Materi

- Pengertian Cyber Crime
- Karakter Cyber Crime
- Jenis Cyber Crime
- Faktor Penyebab Cyber Crime
- Dampak Cyber Crime terhadap Keamanan

# Pengertian Cyber Crime

- Cyber Crime: sebuah evolusi kejahatan
- Jenis kejahatan “konvensional”:
  - a. Kejahatan kerah biru (*blue collar crime*)
    - Spt: pencurian, penipuan, pembunuhan
  - b. Kejahatan kerah putih (*white collar crime*)
    - Spt: Kejahatan korporasi, kejahatan korporat, malpraktek, dll.

# Pengertian Cyber Crime...

- Cybercrime merupakan bentuk<sup>2</sup> kejahatan yg ditimbulkan krn pemanfaatan teknologi internet.
- Cybercrime : dpt didefinisikan sbg perbuatan melawan hukum yg dilakukan dgn menggunakan internet yg berbasis pd kecanggihan teknologi komputer dan telekomunikasi.

# Karakter Unik dari Cyber Crime

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

# 1. Ruang Lingkup Kejahatan

- Cybercrime sering dilakukan secara transnasional, melintasi batas antar negara sehingga sulit dipastikan yuridiksi hukum negara mana yang berlaku terhadapnya.
- Karakteristik internet dimana orang dapat berlalu-lalang tanpa identitas (*anonymous*) sangat memungkinkan terjadinya berbagai aktivitas jahat yang tak tersentuh hukum.

## 2. Sifat Kejahatan

- Sifat kejahatan didunia maya adalah *non-violence*, yaitu tidak menimbulkan kekacauan yg mudah terlihat.
- Jika kejahatan konvensional seringkali menimbulkan kekacauan, maka kejahatan di internet bersifat sebaliknya.
- Shg ketakutan atas kejahatan (*fear of crime*) tsb tidak mudah timbul meskipun bisa saja kerusakan yg diakibatkannya dpt lebih dahsyat dari kejahatan lain.



# 3. Pelaku Kejahatan

- Jika pelaku kejahatan konvensional mudah diidentifikasi dan memiliki tipe tertentu, maka pelaku cybercrime bersifat lebih universal meski memiliki ciri khusus, yaitu kejahatan dilakukan oleh orang<sup>2</sup> yg menguasai penggunaan internet beserta aplikasinya.
- Pelaku kejahatannya tidak terbatas pd usia dan stereotip tertentu, mrk yg sempat tertangkap kebanyakan remaja, bahkan ada yg masih anak<sup>2</sup>.
- Mereka jarang terlibat kenakalan remaja, dari keluarga baik<sup>2</sup>, dan rata<sup>2</sup> cerdas, namun juga jauh dari profil anak jalanan.
- Untuk menangani anak<sup>2</sup> semacam ini, memerlukan pendekatan tersendiri.

## 4. Modus Operandi Kejahatan

- Keunikan dari kejahatan ini adalah penggunaan teknologi informasi dlm modus operandi.
- Itulah sebabnya mengapa modus operandi dlm dunia maya tsb sulit dimengerti oleh orang<sup>2</sup> yg tidak menguasai pengetahuan ttg komputer, teknik pemrogramannya, dsb.
- Sifat inilah yg membuat cybercrime berbeda dgn tindak<sup>2</sup> pidana lainnya.

# 5. Jenis Kerugian yang Ditimbulkan

- Kerugian yg ditimbulkan dr kejahatan ini dpt bersifat material maupun non-material, spt waktu, nilai, jasa, uang, barang, harga diri, martabat, dan bahkan sampai pd kerahasiaan informasi.
- Cybercrime berpotensi menimbulkan kerugian pd banyak bidang spt politik, ekonomi, sosial budaya.
- Dimasa mendatang, kejahatan semacam ini dpt mengganggu perekonomian nasional melalui jaringan infrastruktur yg berbasis teknologi elektronik (perbankan, telekomunikasi satelit, jaringan listrik dan jaringan lalu lintas penerbangan)

# Jenis Cyber Crime

## A. Berdasarkan Jenis Aktivasnya:

### 1. **Unauthorized Access**

- Terjadi ketika seseorang memasuki/menyusup ke dalam suatu sistem jaringan komputer scr tidak sah, tanpa izin / tanpa sepengetahuan dari pemilik sistem jaringan komputer yg dimasukinya.
- Contoh dari kejahatan ini spt: **Probing** dan **Port Scanning**.
- Aktivitas “**Port Scanning**” atau “**Probing**” dilakukan utk melihat servis<sup>2</sup> apa saja yg tersedia di server target.

# Jenis Cyber Crime

## 2. Illegal Contens

- Merupakan kejahatan yg dilakukan dgn memasukkan data / informasi ke internet ttg sesuatu hal yg tidak benar, tidak etis dan dpt dianggap melanggar hukum atau mengganggu ketertiban um

## 3. Penyebaran Virus secara sengaja

- Penyebaran virus umumnya dilakukan dgn menggunakan email.
- Seringkali orang dgn sistem emailnya terkena virus tdk menyadari hal ini.
- Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.
- contoh: kasus: virus Mellisa, I Love You dan Sircam

# Jenis Cyber Crime

## 4. Data Forgery

- Kejahatan jenis ini bertujuan utk memalsukan data pd dokumen<sup>2</sup> penting yg ada di internet.

## 5. Cyber Espionage, Sabotage and Extortion

- **Cyber espionage:** Merupakan kejahatan yg memanfaatkan jaringan internet utk melakukan kegiatan mata<sup>2</sup> terhadap pihak lain dgn memasuki sistem jaringan komputer pihak sasaran.
- Selanjutnya, **sabotage** and **extortion** merupakan jenis kejahatan yg dilakukan dgn membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yg terhubung dgn internet.

# Jenis Cyber Crime

## 6. Cyberstalking

- Dilakukan utk mengganggu atau melecehkan seseorang dgn memanfaatkan komputer, misal. Menggunakan e-mail dan dilakukan berulang<sup>2</sup>.
- Kejahatan tsb menyerupai teror yg ditujukan kpd seseorang dgn memanfaatkan media internet.

## 7. Carding

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

# Jenis Cyber Crime...

## 8. Hacking and Cracking

- Istilah **hacker** biasanya mengacu pd seseorang yg mempunyai minat besar utk mempelajari sistem komputer scr detail dan bagaimana meningkatkan kapabilitasnya.
- Besarnya minat yg dimiliki seorang **hacker** dpt mendorong utk memiliki kemampuan penguasaan sistem **di atas rata<sup>2</sup> pengguna**.
- Jadi, **hacker** memiliki konotasi yg **netral**.
- Mereka yg sering melakukan aksi<sup>2</sup> perusakan di internet lazimnya disebut **cracker**.
- Boleh di bilang para **cracker** ini sebenarnya adalah **hacker** yg memanfaatkan kemampuannya utk hal<sup>2</sup> yg negatif.
- Aktivitas **cracking** di internet memiliki lingkup yg sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran.



# Jenis Cyber Crime

## 9. Cybersquatting and Typosquatting

- **Cybersquatting:** kejahatan yg dilakukan dgn mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kpd perusahaan tsb dgn harga yg lebih mahal.
- **Typosquatting:** kejahatan dgn membuat domain plesetan yaitu domain yg mirip dgn nama domain orang lain.

## 10. Cyber Terrorism

- Suatu tindakan cybercrime termasuk cyber terrorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer.

# Jenis Cyber Crime...

## B. Berdasarkan Motif Keegiatannya:

### 1. Sebagai tindakan murni kriminal

- Kejahatan yg murni merup. tindak kriminal yg dilakukan krn **motif kriminalitas**.
- Kejahatan jenis ini biasanya menggunakan **internet** hanya **sbg sarana kejahatan**.
- Contoh kejahatan semacam ini adalah **carding**.



### 2. Cybercrime sebagai kejahatan “abu-abu”

- Pada jenis kejahatan di internet yg masuk dlm wilayah “**abu-abu**” **cukup sulit** menentukan apakah itu **merupakan tindak kriminal atau bukan**, mengingat motif keegiatannya terkadang bukan utk berbuat kejahatan.
- Contohnya adalah **probing** atau **portscanning**.

# Jenis Cyber Crime...

## C. Berdasarkan Sasaran Kejahatannya

### 1. Menyerang Individu (Against Person)

- Jenis kejahatan ini, sasaran serangannya ditujukan kpd perorangan / individu yg memiliki sifat / kriteria tertentu sesuai tujuan penyerangan tsb.
- Beberapa contoh kejahatan ini antara lain:
  - 1) **Pornografi**
    - Kegiatan yg dilakukan dgn membuat, memasang, mendistribusikan dan menyebarkan material yg berbau pornografi, cabul, serta mengekspos hal-hal yg tidak pantas.
  - 2) **Cyberstalking**
    - Kegiatan yg dilakukan utk mengganggu / melecehkan seseorang misal dgn menggunakan e-mail yg dilakukan scr berulang<sup>2</sup> spt halnya teror di dunia maya.
  - 3) **Cyber Tresspass**
    - Kegiatan yg dilakukan melanggar area privasi orang lain.
    - Misal. Web hacking, breaking the PC, probing, port scanning, dsb.

# Jenis Cyber Crime...

## **2. Menyerang Hak Milik (Against Property)**

- Cybercrime yg dilakukan utk mengganggu / menyerang hak milik orang lain.
- Contoh: carding, cybersquatting, typosquatting, hijacking, data forgery.

## **3. Menyerang Pemerintah (Against Government)**

- Cybercrime Against Government dilakukan dgn tujuan khusus penyerangan terhadap pemerintah.

# Faktor yang Mempengaruhi Terjadinya Cyber Crime

## 1. Faktor Politik

- Kebijakan politik pemerintah Indonesia sangat diperlukan utk menanggulangi *cybercrime* yg sudah berkembang di Indonesia.
- Aparat penegak hukum telah berupaya keras utk menindak setiap pelaku *cybercrime*, tapi penegakkan hukum **tidak dapat berjalan maksimal** krn perangkat hukum yg mengatur khusus tentang *cybercrime* **belum ada**.

## 2. Faktor Ekonomi

- Kemajuan ekonomi suatu bangsa salah satunya dipengaruhi oleh promosi barang<sup>2</sup> produksi.
- Jaringan komputer dan internet merupakan media yg sangat murah utk promosi.
- Seluruh komponen bangsa Indonesia harus berpartisipasi utk mendukung pemulihan ekonomi akibat dari krisis ekonomi.
- Media internet dpt dimanfaatkan oleh seluruh masyarakat utk mempromosikan Indonesia.

# Faktor yang Mempengaruhi Terjadinya Cyber Crime

## 3. Faktor Sosial Budaya

Ada beberapa aspek utk faktor sosial budaya:

### a) Kemajuan Teknologi Informasi

- Era globalisasi, manusia tdk akan bisa melepaskan kebutuhan akan TI.
- Dengan teknologi informasi manusia dpt melakukan akses perkembangan lingkungan scr akurat.

### b) Sumber Daya Manusia

- Sumber daya manusia dlm teknologi informasi mempunyai peranan penting sbg pengendali dari sebuah alat.
- Apakah ala itu digunakan sbg sarana kebajikan ataukah akan dikriminalisasikan shg dpt merusak kepentingan orang lain/bahkan negara.

### c) Komunitas Baru

- Dengan adanya media internet sbg wahana utk berkomunikasi, scr sosiologis terbentuklah komunitas baru di dunia maya yakni komunitas para pengguna internet yg saling berkomunikasi.
- Misal. Mailing List, Forum, Chatting, dsb.

# Dampak Cyber Crime terhadap Keamanan Negara

## 1. Kurangnya kepercayaan dunia thd Indonesia

- Kasus cybercrime yg terungkap di Bandung, ada 7 pelaku carding, pembobol kartu kredit melalui internet.
- Dengan adanya kejahatan tsb dpt menurunkan citra dan nama baik bangsa Indonesia, krn pemesanan brg melalui internet E-Business dr berbagai negara dilakukan dgn kartu kredit palsu.

## 2. Berpotensi menghancurkan negara

- Tak ada satu negara di dunia ini yg terbebaskan dr ancaman cybercrime.
- Pencegahan thdp tindakan cybercrime hrs mencakup semua operasi illegal yg dpt merugikan pihak lain.
- Contoh yg terjadi pd jaringan KPU pd saat penghitungan suara.

# Dampak Cyber Crime terhadap Keamanan Dalam Negeri

- **Kerawanan sosial dan politik** yg ditimbulkan dr cybercrime antara lain: isu<sup>2</sup> yg meresahkan, memanipulasi simbol<sup>2</sup> kenegaraan, dan partai politik dgn tujuan utk mengacaukan keadaan agar tercipta suasana yg tdk kondusif.
- **Munculnya pengaruh negatif** dr maraknya situs<sup>2</sup> porno yg dpt diakses bebas tanpa batas yg dpt merusak moral bangsa.
- **Ulah par hacker yg meraih keuntungan scr finansial** dgn merusak situs<sup>2</sup> perbankan, kartu kredit lembaga-keuangan dgn maksud terjadinya kekacauan dlm bidang perdagangan.



# Menuju UU Cyber Republik Indonesia

## **Strategi penanggulangan CyberCrime:**

- a. Strategi Jangka Pendek
- b. Strategi Jangka Menengah
- c. Strategi Jangka Panjang

# Menuju UU Cyber Republik Indonesia...

## a. Strategi Jangka Pendek

### 1. Penegakan Hukum Pidana

- Penegakan hukum pidana adalah salah satu manifestasi utk membuat hukum tdk hanya sbg barang rongsokan yg tak berguna.

### 2. Mengoptimalkan UU Khusus Lainnya

- Sektor cyberspace, jg banyak bersentuhan dgn sektor<sup>2</sup> lain yg telah memiliki aturan khusus dlm pelaksanaannya.
- Ada bbrp aturan yg bersentuhan dgn dunia cyber yg dpt dig. utk menjerat pelaku cyber crime shg sepak terjang mrk semakin sempit.

### 3. Rekrutmen Aparat Penegak Hukum

- Diutamakan dr masyarakat yg menguasai dunia komputer & internet disamping kemampuan lain yg dipersyaratkan.

# Menuju UU Cyber Republik Indonesia...

## b. Strategi Jangka Menengah

### 1. Cyber Police

- Cyber Police merup. orang<sup>2</sup> khusus yg dilatih dan didik utk melakukan penyidikan cyber crime.
- Pola pembentukan cyber police merup. Bagian bagian dr upaya reformasi kepolisian.
- Sayangnya pola yg ada saat ini, belum dilakukan scr sistematis dlm struktur Polri, hanya br ada di Mabes Polri dan Polda Metro, padahal kejahatan dunia maya ada di berbagai tempat.

### 2. Kerjasama Internasional

- Kerjasama kepolisian internasional perlu ditindaklanjuti utk melakukan penegakan hukum, krn kejahatan modern sdh melintasi batas<sup>2</sup> negara yg dilakukan berkat dukungan teknologi, sistem komunikasi & transportasi.
- Kerjasama internasional dpt menunjukkan adanya sistem kepolisian yg terbuka dan bisa mendptkan keuntungan dlm kerjasama mengatasi penjahat<sup>2</sup> internasionala yg masuk melintasi wilayah hukum Indonesia.

# Menuju UU Cyber Republik Indonesia...

## **b. Strategi Jangka Panjang**

### **1. Membuat UU Cyber Crime**

- Tujuan pembuatan UU yg khusus mengatur ttg dunia maya ini adl utk pemberatan atas tindakan pelaku agar dpt menimbulkan efek jera dan mengatur sifat khusus dr sistem pembuktian.
- Dgn adanya UU yg khusus mengatur cyber crime maka dpt mempermudah aparat penegak hukum dlm penegakan hukum.

### **2. Membuat Perjanjian Bilateral**

- Indonesia merupk bagian dr tata pergaulan dunia.
- Media internet adl media global, yg tdk ada batasan waktu dan tempat.
- Cyber crime melibatkan bbrp negara, shg perlu hubungan di jalur bilateral utk menanggulangnya.
- Tidak2 semua negara memiliki hub. Blateral dgn Indonesia, mk scr politis perlu dilakukan upaya utk menjadlin hubungan yg dimaksud.

**Sekian...**

# Tugas:

- Setiap mahasiswa mencari contoh kasus cyber crime yang pernah terjadi di Indonesia / dunia.
- Berikan deskripsi kasus, termasuk dalam jenis cyber crime yang manakah dan status/penyelesaian kasus tersebut.
- Jangan lupa sertakan referensi pustaka sebagai sumber kasus.
- Kumpulkan Tugas dalam bentuk hardcopy minggu depan sebagai pengganti tatap muka **akhir bulan MEI**.