Internet sudah bukan menjadi sesuatu yang baru lagi bagi kita. Keberadaannya di tengah-tengah masyarakat sangatlah membantu dalam menjalani kehidupan sehari-hari manusia. Kebutuhan akan internet sudah menjadi candu yang sulit dihentikan. Hal ini menyebabkan perkembangan dan perubahan dalam hal ekonomi sampai hal yang bersifat social. Perkembangan yang sangat pesat ini menimbulkan berbagai dampak, baik yang positif maupun negatif. Hal negatif ini disebabkan oleh banyaknya kejahatan dunia maya atau yang sering disebut cybercrime.

Banyak sekali jenis-jenis cybercrime (kejahatan dunia maya) yang sering terjadi di tengah semakin meningkatnya pengguna internet oleh manusia. Dalam makalah ini, penulis akan mengangkat masalah cybercrime yang ada pada social networking ataupun kejahatan dunia maya yang ada.

Makalah ini dibuat oleh penulis untuk melengkapi tugas mata kuliah Etika Profesi, selain itu makalah ini juga dibuat untuk memberikan informasi yang mungkin berguna bagi pembaca. Ucapan terima kasih penulis sampaikan kepada seluruh pihak yang telah membantu dalam menyelesaikan tugas ini.

**BAB I**

**PENDAHULUAN**

* 1. **Latar belakang**

Kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dengan Internet dalam segala bidang seperti e-banking, e-commerce, e-government,e-education dan banyak lagi telah menjadi sesuatu yang lumrah. Bahkan apabila masyarakat terutama yang hidup di kota besar tidak tersentuhan dengan persoalan teknologi informasi dapat dipandang terbelakang atau ”GAPTEK”. Internet telah menciptakan dunia baru yang dinamakan cyberspace yaitu sebuah dunia komunikasi berbasis computer yang menawarkan realitas yang baru berbentuk virtual (tidak langsung dan tidak nyata).

Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik positif maupun negatif. Tentunya untuk yang bersifat positif kita semua harus mensyukurinya karena banyak manfaat dan kemudahan yang didapat dari teknologi ini, misalnya kita dapat melakukan transaksi perbankan kapan saja dengan e-banking, e-commerce juga membuat kita mudah melakukan pembelian maupun penjualan suatu barang tanpa mengenal tempat. Mencari referensi atau informasi mengenai ilmu pengetahuan juga bukan hal yang sulit dengan adanya e-library dan banyak lagi kemudahan yang didapatkan dengan perkembangan Internet. Tentunya, tidak dapat dipungkiri bahwa teknologi Internet membawa dampak negatif yang tidak kalah banyak dengan manfaat yang ada. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian dan penipuan kini dapat dilakukan dengan menggunakan media komputer secara online dengan risiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun Negara disamping menimbulkan kejahatan-kejahatan baru. Banyaknya dampak negatif yang timbul dan berkembang, membuat suatu paradigma bahwa tidak ada computer yang aman kecuali dipendam dalam tanah sedalam 100 meter dan tidak memiliki hubungan apapun juga

Dalam dunia maya (internet), masalah keamanan adalah satu hal yang sangat diperlukan. Karena tanpa keamanan bisa saja data-data dan sistem yang ada di internet bisa dicuri oleh orang lain. Seringkali sebuah sistem jaringan berbasis internet memiliki kelemahan atau sering disebut juga lubang keamanan (hole). Nah, kalau lubang tersebut tidak ditutup, pencuri bisa masuk dari lubang itu. Pencurian data dan sistem dari internet saat ini sudah sering terjadi. Kasus ini masuk dalam kasus kejahatan komputer. Istilah dalam bahasa Inggrisnya : Cybercrime.

* 1. **Tujuan**

Untuk meluruskan salah kaprah tentang pengertian hacker yang benar dan janganlah menjadi cracker yang berbahaya dan tidak ada gunanya. Di masyarakat umum, istilah hacker ini banyak tersalahgunakan atau rancu dengan istilah Cracker. Dimana sering para pecinta teknologi yang merasa dirugikan langsung mengasumsikan bahwa si hacker inilah biang keroknya.

* 1. **Pokok – pokok Masalah**

Cybercrime adalah kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi cyber dan terjadi di dunia cyber. Banyak diantaramya adalah pegawai sebuah perusahaan yang loyal dan dipercaya oleh perusahaan-nya, dan dia tidak perlu melakukan kejahatan computer. Mereka adalah orang-orang yang tergoda pada lubang-lubang yang terdapat pada sistem computer. Sehingga kesempatan merupakan penyebab utama orang-orang tersebut menjadi ‘penjahat cyber’. Kategori Cybercrime adalah :

1. Cyberpiracy

Penggunaan teknologi komputer untuk :

* + mencetak ulang software atau informasi
  + mendistribusikan informasi atau software tersebut melalui jaringan computer

1. Cybertrespass

Penggunaan teknologi komputer untuk meningkatkan akses pada:

* + Sistem komputer sebuah organisasi atau individu
  + Web site yang di-protect dengan password

1. Cybervandalism

Penggunaan teknologi komputer untuk membuat program yang :

* + Mengganggu proses transmisi informasi elektronik
  + Menghancurkan data di computer

**BAB II**

**PEMBAHASAN**

**2.1. Pengertian Cyber Crime**

Cyber Crime 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, confidence fraud, penipuan identitas, pornografi anak, dll.

Walaupun kejahatan dunia maya atau cybercrime umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Contoh kejahatan dunia maya di mana komputer sebagai alat adalah spamming dan kejahatan terhadap hak cipta dan kekayaan intelektual. Contoh kejahatan dunia maya di mana komputer sebagai sasarannya adalah akses ilegal (mengelabui kontrol akses), malware dan serangan DoS. Contoh kejahatan dunia maya di mana komputer sebagai tempatnya adalah penipuan identitas. Sedangkan contoh kejahatan tradisional dengan komputer sebagai alatnya adalah pornografi anak dan judi online.

**2.2. Karakteristik Cyber Crime**

Selama ini dalam kejahatan konvensional, dikenal dengan adanya dua jenis kejahatan sebagai berikut :

* Kejahatan Kerah Biru (blue collar crime)
* Kejahatan Kerah Putih (white collar crime)

Cybercrime memiliki karakteristik unik yaitu :

1. Ruang lingkup kejahatan

2. Sifat kejahatan

3. Pelaku kejahatan

4. Modus kejahatan

5. Jenis kerugian yang ditimbulkan

Dari beberapa karakteristik diatas, untuk mempermudah penanganannya maka cyber crime diklasifikasikan :

* Cyberpiracy : Penggunaan teknologi computer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
* Cybertrespass : Penggunaan teknologi computer untuk meningkatkan akses pada system computer suatu organisasi atau indifidu.
* Cybervandalism : Penggunaan teknologi computer untuk membuat program yang menganggu proses transmisi elektronik, dan menghancurkan data dikomputer

**2.3. Faktor-faktor Penyebab Cyber Crime**

Adapun yang menjadi penyebab terjadinys cybercrime antara lain;

1. Akses internet yang tidak terbatas
2. Kelalaian pengguna komputer. Hal ini merupakan salah satu penyebab utama kejahatan komputer.
3. Mudah dilakukan dengan alasan keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sulit untuk melacakny, sehingga ini mendorong para pelaku kejahatan untuk terus melakukan hal ini.
4. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh diatas operator komputer.
5. Sistem keamanan jaringan yang lemah
6. Kurangnya perhatian masyarakat dan penegak hukum.

**2.4. Penanggulangan Cyber Crime**

Fenomena cybercrime memang harus di waspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya yang dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan.

Aktivitas pokok dari cybercrime adalah penyerangan terhadap content, computer system dan communication system milik orang lain atau umum didalam cyberspace. Fenomena cybercrime memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya.

Cybercrime dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dan korban kejahatan.

Berikut ini cara penanggulangannya :

1. Mengamankan system

Tujuan yang nyata dari sebuah sistem keamanan adalah mencegah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem secara terintegrasi sangat diperlukan untuk meminimalisasikan kemungkinan perusakan tersebut. Membangun keamanan sebuah sistem harus merupakan langkah-langkah yang terintegrasi pada keseluruhan subsistemnya, dengan tujuan dapat mempersempit atau bahkan menutup adanya celah-celah unauthorized actions yang merugikan. Pengamanan secara personal dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya menuju ketahap pengamanan fisik dan pengamanan data. Pengaman akan adanya penyerangan sistem melalui jaringan juga dapat dilakukan dengan melakukan pengamanan FTP, SMTP, Telnet dan pengamanan web server.

1. Penanggulangan Global

The Organization for Economic Cooperation and Develoment (OECD) telah membuat guidelines bagi para pembuat kebijakan yang berhubungan dengan computer-related crime,dimana pada tahun 1986 OECD telah memublikasikan laporannya yang berjudul “Computer-Related Crime: Analisis of Legal Policy”.

Menurut OECD, beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime adalah:

1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya.
2. Mengamankan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime.
4. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.
5. Meningkatkan kerjasama antarnegara, baik bilateral, regional, maupun multilateral, dalam upaya penanganan cybercrime.

Pemerintah juga telah berupaya untuk menanggulangi semakin maraknya cybercrime dengan diberlakukannya aspek-aspek hukum kejahatan didunia maya antara lain:

1. Asas subjective territoriality

Asas yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.

1. Asas objective territoriality

Asas yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan

1. Asas nasionality

Asas yang menentukan bahwa negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan keswarganegaraan pelaku.

1. Asas protective principle

Asas yang menekankan jurisdiksi berdasarkan kewarganegaraan korban.

1. Asas universality

Asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan

Berikut ini akan dibahas beberapa hal pokok yang dapat dilakukan dalam upaya menanggulangi merebaknya kejahatan internet.

1. Mengamankan sistem

Keamanan komputer identik dengan suatu tindakan baik pencengahan maupun pendeteksian terhadap kegiatan –kegiatan yang tidak mendapat izin oleh pemakai maupun sistem komputer. Adapun pada pandangan makro, keamanan data bukan saja menyangkut masalah teknis belaka, tetapi memiliki konsep yang lebih luas dan berkaitan dengan ketergantungan suatu institusi terhadap institusi lainnya, atau bahkan suatu negara terhadap negara lainnya. Keamanan juga penting untuk membangun kepercayaan ( trust ) terhadap sebuah sistem secara umum.

Tujuan yang paling nyata dari sebuah sistem keamanan adalah mencengah adanya perusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem secara terintegrasi sangat diperlukan untuk meminimalisasi kemungkinan kerusakan tersebut.

1. Penanggulangan Global

Saat ini berbagai upaya telah dipersiapkan untuk memerangi cybercrime. The Organisation for Economic Cooperation and Development (OECD) telah membuat guidelines bagi para pembuat kebijakan yang berhubungan dengan computer-related crime, dimana pada tahun 1986 OEDC telah mempublikasikan laporannya yang berjudul computer-related crime: Analist of Legal Policy.

Laporan OECD tersebut berisi hasil survei terhadap peraturan perundang-undangan negara-negara anggota beserta rekomendasi perubahannya dalam menanggulangi computer-related crime tersebut, yang mana diakui bahwa sistem telekomunikasi juga memiliki peran penting dalam kejahatan tersebut. Dari berbagi upaya yang dilakukan tersebut, jelas bahwa cybercrime membutuhkan global action dalam penanggulangannya mengingat kejahatan tersebut sering kali bersifat transnasional.

Menurut OECD, beberapa langkah penting yang harus dilakukan setiap negara dalam penanggulangan cybercrime adalah:

* 1. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
  2. Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.
  3. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntunan perkara-perkara yang berhubungan dengan cybercrime.
  4. Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi.
  5. Meningkatkan kerja sama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime, antara lain melalui perjanjian ekstradisi dan mutual assistance treaties.

1. Perlunya Cyberlaw

Perkembangan teknologi yang sangat pesat membutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut. Sayangnya, hingga saat ini banyak negara (termasuk indonesia) belum memiliki perundang-undangan khusus dibidang teknologi informasi, baik dalam aspek pidana maupun perdatanya. Ketertinggalan perundang-undangan dalam menyesuaikan diri dengan kemajuan teknologi informasi tersebut menuntut adanya solusi sementara untuk mengatasi cybercrime, yakni melalui terobosan keputusan pengadilan. Ini tentu saja mensyaratkan adanya sosok hakim yang kreatif, berwawasan teknologi, dan berani melakukan terobosan melalui keputusannya.

Banyak kasus yang membuktikan bahwa perangkat hukum di bidang TI masih lemah. Seperti contoh, masih belum diakuinya dokumen elektronik secara tegas sebagai alat bukti oleh KUHAP. Hal tersebut dapat dilihat pada UU No8/1991 pasal 184 ayat 1 bahwa UU ini secara definitif membatasi alat-alat bukti hanya sebagai keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwah saja.

1. Perlunya dukungan lembaga khusus

Lembaga-lembaga khusus, baik milik pemerintah maupun NGO (non government organisation), diperlukan sebagai upaya penanggulangan kejahatan di internet. Amerika Serikat memiliki Computer Crime and Intellectual Property Section (CCIPS) sebagai divisi khusus dari U.S. Departement of Justice. Institusi ini memberikan informasi tentang cybercrime, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan cybercrime.

Terdapat pula National Infrastructure Protection Center (NIPC) sebagai institusi di Amerika Serikat yang menangani masalah yang berhubungan dengan infrastruktur. Institusi ini mengidentifikasi bagian infrastruktur yang penting (critical) bagi negara (khususnya bagi negara Amerika Serikat). Internet atau jaringan komputer sudah dianggap sebagai infrastruktur yang perlu mendapat perhatian khusus. Institusi ini juga memberikan advisory bagi setiap orang yang memerlukan solusi atas kejahatan di bidang komputer.

Indonesia sendiri sebenarnya sudah memiliki IDCERT (Indonesia Computer Emergency Response Team). Unit ini merupakan point of contact bagi orang untuk melaporkan masalah-masaslah keamanan komputer.