**Modul Pertemuan Sesi 6**

**Mata Kuliah Kriminologi dan Viktimologi**

***Disusun oleh: Idris Wasahua***

**Materi : Tipologi Kejahatan**

Tipologi merupakan suatu sistem klasifikasi kejahatan atau penjahat ke dalam golongan atau kelompok tertentu, lazimnya dibedakan menjadi tipologi teoritis dan tipologi empiris. Tipologi penjahat diklasifikasi berdasarkan umur, jenis kelamin, kepribadian, status maritalm motif, kelas sosial dan sebaginya.

Tipologi kejahatan diklasifikasi berdasarkan motif, kondisi perilaku, kaidah yang dilanggar frekuensi kejahtaan dan sebagainya.  
Adapun yang diuraikan disini adalah tipologi kejahatan yang berguna untuk pembahasan selanjutnya terutama dalam membahas tentang penaggulangan pelanggar hukum. Misalnya menanggulangi pemabuk akan berbeda dengan menanggulangi perampok.

Walter C. Recless membedakan karir penjahat ke dalam 3 jenis :

**1. Penjahat biasa**

Merupakan peringkat terendah dalam karir kriminil. Penjahat jenis ini melakukan kejahatan konvensional mulai dari pencurian ringan sampai pencurian dengan kekerasan yang membutuhkan keterampilan terbatas, serta kurang mempunyai organisasi.

**2. Penjahat terorganisasi**

Tipe penjahatan ini pada umumnya memiliki organisasi yang kuat dan dapat menghindari penyelidikan, serta mengkhususkan diri dalam bisnis ilegal berskala besar, Kekuatan, kekerasan, intimidasi dan pemerasan digunakan untuk memperoleh dan mempertahankan pengendalian atas kegiatan ekonomi diluar hukum

Faktor Penyebab Kejahatan terorganisir terjadi karena berbagai factor, antara lain:

Kurangnya kemampuan untuk melakukan sesuatunya sendiri, mudah tergoda ajakan orang lain, masalah ekonomi keluarga, adanya kesalahpahaman, adanya masalah/dendam dengan sekelompok orang.

Organisasi kejahatan tersebut cukup canggih sehingga tidak mudah terdeteksi. Organisasi kejahatan tersebut cepat menyesuaikan diri mengikuti perkembangan teknologi penyidikan penegakhukum. Organisasi kejahatan memegang penegak hukum dan pejabat pemerintah dedngan cara menyuap. Organisasi kejahatan membunuh penegak hukum dan pejabat pemerintah yang tidak bisa disuap. Penegak hukum dan pejabat pemerintah takut dengan ancaman pembunuhan oleh organisasi kejahatan. Para anggota organisai kejahatan menjalankan kewajibannya (perintah atasan) dengan disiplinyang tinggi.

Untuk dapat mengatasi kejahatan terorganisasi diperlukan tekad dan semangat yang kuat dari penegak hukumdan pemerintah. Integritas para penegak hukum dan pemerintah yang tinggi sehingga tidak gampang disuap oleh para mafia. Adanya keberanian dari penegak hukum dan pemerintah sehingga tidak takut dari ancaman para mafia, termasuk ancaman pembunuhan. Adanya undang-undang yang dapat benar-benar menunjang pembasmian para mafia. Menggunakan seefektif mungkin para informan yang berasaldari anggota mafia yang membelot. Keikutsertaan masyarakat untuk membasmi mafia, dengan tidak menyembunyikan data para mafia dan beran melaporkannya kepada pihak berwajib

**3. Penjahat Professional**

Lebih mempunyai kemahiran yang tinggi dan mampu menghasilkan kejahatan yang besar dan sulit diungkapkan oleh penegak hukum. Penjahat-penjahat jenis ini mengkhususkan diri dalam kejahatan-kejahatan yang lebih membutuhkan keterampilan daripada kekerasan.

**Tipe Penjahat Menurut Bonger :**

***The Cassual Offender***

Tipe ini sebenarnya belum dapat disebut penjahat, tetapi pelanggar kecil, seperti tidak pakai lampu pada malam hari atau tidak berjalan di sisi kiri jalan.

***The Occasional Criminal***

Orang ini melakukan kejahatan ringan seperti, orang yang menabrak sehingga korban luka ringan.

***The Episodic Criminal***

Perbuatannya disebabkan karena emosi yang hebat, sehingga dia kehilangan kontrol.

***The Habitat Criminal***

Mereka atau orang yang selalu mengulangi perbuatannya, seperti pemabok, pengemis. Dan dapat juga digolongkan sebagai residivis.

***The Professional Criminal***

Pelaku perbuatan ini sebagai mata pencaharian, karena sifatnya mata pencaharian tentunya banyak terjadi di lapangan ekonomi seperti penyelundupan, korupsi, penjualan narkotik.

***Organized Crime***

Para pelaku mengadakan organisasi yang rapi untuk operasi kejahatan.

***Ciri organized crime modern menurut Clinnard dan Quinney :***

* Mempunyai struktur hirarki dengan pola hubungan yang bermutual dan previlese
* Mengendalikan monopoli atau membangun pengaruh terhadap kelompok/wilayah lain
* Menggantungkan diri pada penggunaan kekerasan dalam menegakkan disiplin dan menghadapi pesaing
* Memelihara kekebalan hukum
* Memperoleh keuntungan yang luar biasa besar.

* ***The Mentally Abnormal Criminal***

Penjahat ini menderita penyakit psikopatis dan psikotis, penjahat yang mengalami gangguan jiwa.

* ***The Nonmalicious Criminal***

Sesuatu perbuatan dinilai sekolompok masyarakat sebagai kejahatan sedang kelompok lain menyebut bukan kejahatan. Kejahatan ini bersifat relatif. Ada orang yang menuduh seorang laki’ menyerahkan isterinya pada tamunya sebagai kejahatan. Hal ini dilakukan sebagai adat istiadat mereka dalam menyambut tamunya.

* ***The White Collar Crime***

Kejahatan yang dilakukan oleh seorang dari **upper class** didalam rangka melaksanakan kegiatan-kegiatan dalam jabatan, baik di bidang ekonomi maupun sosial politik dan terutama merupakan pelanggaran atas kepercayaan dari masyarakat kepadanya. Kerugian yang ditimbulkan bersifat materi dan immateril. Yang dimaksud immateril timbulnya ketidakpercayaan dan menurunnya kepercayaan masyarakat kepadanya.

Kejahatan kerah putih atau white collar crime merupakan suatu tindak kecurangan yang dilakukan oleh seseorang yang memiliki posisi dan wewenang cukup tinggi pada sektor pemerintahan maupun sektor swasta, sehingga dapat mempengaruhi suatu kebijakan dan keputusan. Bicara mengenai white collar crime memang cukup luas ranah pembahasannya, dimana terkadang terjadi beberapa pendapat ahli yang berbeda terkait scopedari masing-masing kejahatan apakah bisa diklasifikasikan sebagai white collar crime atau bukan. Menurut Edwin H. Sutherland, white collar crime merupakan kejahatan yang dilakukan oleh seseorang yang sangat terhormat dan berstatus social tinggi di dalam pekerjaannya. Tindakan kejahatan ini dapat terjadi di dalam perusahaan, kalangan professional, perdagangan maupun kehidupan politik.

Dalam memahami white collar crime, diperlukan pengetahuan terkait tipologi pelaku kejahatan tersebut. Sebab, definisi terkait suatu tindak kejahatan dapat digolongkan ke dalam white collar crime atau tidak dapat dilihat berdasarkan tipologi pelakunya. Tipologi pertama dilihat dari status social pelaku, apakah berasal dari status “terhormat” atau tidak. Status terhormat dalam hal ini merupakan suatu jabatan yang dimiliki pelaku dalam instansi, baik negera maupun swasta, yang ia miliki. Selanjutnya, tipologi yang dapat dilihat adalah tindak kejahatan yang dilakukan memerlukan keahlian di bidang komputerisasi atau tidak. Jika, iya, maka kejahatan yang dilakukan dapat digolongkan sebagai WCC dalam lingkup cyber crime. Terakhir, tindak kejahatan yang dilakukan pelaku bertujuan untuk menguntungkan individu atau kelompok. Melalui ini, dapat dilihat pola seleksi dan penggolongan dari kasus white collar crime yang terjadi. Tipologi pelaku white collar crime dapat dilihat melalui gambar bagan berikut.

White collar crime ini pada umumnya terjadi pada negara-negara yang belum memiliki hukum korporat yang matang. Sehingga para pelaku dapat dengan mudah melakukan aksinya tanpa ragu terkait hukuman yang mungkin mereka akan peroleh. Negara dengan kematangan hukum koorporat yang rendah ini banyak terdapat di wilayah Asia, khususnya pada negara-negara berkembang. Meski demikian, tidak menutup kemungkinan juga bahwa pelaku white collar crime berasal dari negara-negara dengan ekonomi tinggi, seperti Jepang dan Cina misalnya. Jepang yang seringkali digambarkan sebagai salah satu negara maju di Asia dengan tingkat kejahatan rendah justru memiliki jumlah kasus white collar crime yang tidak sedikit. Hal ini mengindikasikan bahwa kemungkinan besar, kejahatan umum (street crime) di Jepang ternilai sangat rendah akibat dikalahkan oleh kuantitas kejahatan kerah putih dan korporat yang lebih tinggi dan samar terlihat. Sedangkan di China yang merupakan negara dengan ekonomi tertinggi di Asia, white collar crime lebih banyak dipengaruhi oleh faktor reformasi ekonomi yang berimplementasi pada ketidakstabilan kehidupan ekonomi-politik negara tersebut.

Kasus white collar crime banyak tersebar di berbagai negara di Asia seiring dengan tekanan yang dihasilkan dari kondisi ekonomi saat krisis. Krisis menyebabkan banyak barang yang dipasarkan melebihi dari kapasitas pembeli. Sehingga perputaran uang tidak dapat berjalan lancar. Di asia-pasific hal ini menyebabkan berkurangnya permintaan untuk berbagai area ekspor, khususnya tourism, manufaktur dan komoditas. Dengan ini, pendapatan pemerintah juga menurun drastis, terutama dari pekerja luar negeri. Di era krisis ini, korupsi kemudian menjadi salah satu fenomena yang marak berkembang. Terhambatnya arus perputaran uang di masa krisis menyebabkan banyaknya tawaran hutang luar negeri. Tawaran hutang luar negeri inilah yang banyak dimanfaatkan oleh pelaku white collar crime untuk menjalankan aksinya dengan berbagai bentuk modus kejahatan. Berbagai bentuk white collar crime yang umumnya terjadi di Asia antara lain seperti **korupsi, penyuapan, penipuan, cuci uang, penggunaan asset publik untuk kepentingan pribadi, penjualan gelap, dan penghindaran pajak.**

Di wilayah Asia sendiri white collar crime dapat didefinisikan ke dalam beberapa jenis. Berdasarkan beberapa sumber yang penulis peroleh dari jurnal dan portal berita international, pengklasifikasian white collar crime di Asia seringkali dibedakan berdasarkan ciri khas dari suatu regional tertentu. Misalnya, pada Asia Barat dimana terdapat banyak negara-negara penghasil minyak bumi, kasus white collar crime yang terjadi banyak terafiliasi dengan perusahaan-perusaan offshore tertentu. Misal seperti yang terjadi di Khazakhstan dan Kyrgystan, dimana white collar crime yang banyak terjadi seringkali disampul dalam bentuk fraud (penipuan) yang melibatkan kegiatan ekonomi pada perusahaan-perusahaan offshore. Kemudian, pada negara-negara di wilayah Asia Tenggara yang mayoritas merupakan negara berkembang yang sedang mengedepankan ekonomi pasar terbuka, white collar crime cenderung melibatkan pelaku bisnis dan usahawan, serta tidak sedikit yang berhubungan dengan pemerintah. Seperti yang terjadi di Indonesia misalnya, dimana banyak usahawan yang memiki investasi tinggi melakukan kecurangan berupa tax evasion (penghindaran pajak) yang melibatkan kerjasama dengan oknum-oknum pada institusi pajak. Sedangkan pada negara-negara di kawasan Asia Timur yang tergolong cukup mapan ekonominya, kasus white collar crime yang terjadi sedikit banyak melibatkan perusahaan-perusahaan pendukung ekonomi negara. Misalnya pada Jepang dan Korea Selatan, dimana pemimpin-pemimpin perusahaan ternama, seperti Sharp, Nikon, dan Samsung seringkali terlibat ke dalam kasus tersebut.

Terakhir, pengklasifikasian white collar crime juga dapat dilihat dari peran atau kontrol pemerintah dalam suatu negara. Hal ini berhubungan dengan ranah white collar crime itu sendiri yang selalu terjadi di dalam sektor ekonomi — politik. Dimana pada negara dengan kontrol pemerintah yang tinggi pada kegiatan ekonomi — politik, termasuk produksi, maka white collar crime cenderung terjadi di institusi pemerintahan. Bentuk ini banyak terjadi pada negara-negara berkembang di Asia Tenggara yang kegiatan ekonominya banyak dikelola oleh negara. Sedangkan pada negara yang cenderung melakukan penerapan free-trade dan liberalisasi ekonomi, sektor swasta memiliki peran yang lebih besar dalam kegiatan ekonomi. Sehingga, white collar crime yang banyak terjadi juga berasal dari sektor swasta dan jangkauannya dapat dikatakan sebagai transnasional, terebih jika teknologi di negara tersebut telah maju dan berkembang.

Melalui berbagai pembahasan di atas, dapat disimpulkan bahwa white collar crime merupakan sebuah fenomena kejahatan yang cukup luas, baik terkait definisi maupun pengklasifikasian tindakannya. Dalam memahami white collar crime diperlukan focus pemahan terhadap tipologi pelakunya terlebih dahulu. Dengan ini suatu tindak kejahatan dapat digolongkan ke dalam bentuk white collar crime atau bukan. Di Asia sendiri, white collar crime sudah marak terjadi sejak terjadinya krisis ekonomi yang jelas berpengaruh terhadap penurunan pendapatan negara dan peningkatan hutang yang menjadi lading terjadinya tindak kejahatan ini. White collar crime di Asia juga dapat diidentifikasikan berdasarkan ciri khas dari masing-masing region, seperti Asia Barat dengan white collar crime yang kerap terafiliasi dengan perusahaan offshore dan Asia Tenggara yang kerap melibatkan peran usahawan. Terakhir, white collar crime di Asia juga dapat dilihat berdasarkan peran atau kontrol pemerintah di dalam kegiatan ekonomi dan politik. Dimana pada negara yang kontrolnya tinggi pada kegiatan ekonomi politik, white collar crime banyak terjadi di dalam instansi negara. Sedangkan pada negara yang kegiatan ekonomi politiknya lebih banyak menggunakan peran swasta, white collar crime justru seringkali terjadi pada perusahaan-perusahaan swasta.

*(*[*https://medium.com/@dwitaks/kejahatan-kerah-putih-white-collar-crime-di-*](https://medium.com/@dwitaks/kejahatan-kerah-putih-white-collar-crime-di-)*asia-5199c723601e)*

**Kejahatan Kontemporer**

* **Terorisme**

Adalah serangan-serangan terkoordinasi yang bertujuan membangkitkan perasaan teror terhadap sekelompok masyarakat. Berbeda dengan [perang](https://id.wikipedia.org/wiki/Perang), aksi terorisme tidak tunduk pada tatacara peperangan seperti waktu pelaksanaan yang selalu tiba-tiba dan target korban jiwa yang acak serta seringkali merupakan [warga sipil](https://id.wikipedia.org/wiki/Warga_sipil).

Lebih berkaitan dengan pelaku yg menganut ideologi yg salah. Selain saasarannya pada org banyak, juga terhadap tempat-tempat tertentu yang dipandang strategis

* **Kejahatan Kebencian** (***Hate Crime***)

Merupakan tindak pidana yang dilakukan setidak-tidaknya atau sebagian dengan motivasi adanya kelompok afiliasi korban (Gerstenfeld). Contohnya di Indonesia adalah gerakan pemerintah orde baru yang melakukan program “Ganjang PKI”

* **Kejahatan Transnasional:**

Adalah [kejahatan terorganisasi](https://id.wikipedia.org/w/index.php?title=Kejahatan_terorganisasi&action=edit&redlink=1) yang terjadi lintas perbatasan negara dan melibatkan kelompok atau jaringan yang bekerja di lebih dari satu negara untuk merencanakan dan melaksanakan bisnis ilegal.  Demi mencapai tujuan mereka, kelompok penjahat ini menggunakan kekerasan sistematis dan korupsi. Kejahatan terorganisasi transnasional yang paling lazim adalah [pencucian uang](https://id.wikipedia.org/wiki/Pencucian_uang); [penyelundupan manusia](https://id.wikipedia.org/w/index.php?title=Penyelundupan_manusia&action=edit&redlink=1); [kejahatan siber](https://id.wikipedia.org/w/index.php?title=Kejahatan_siber&action=edit&redlink=1); dan [perdagangan manusia](https://id.wikipedia.org/wiki/Perdagangan_manusia), obat-obatan, senjata, [hewan terancam punah](https://id.wikipedia.org/wiki/Perburuan_liar), organ tubuh, atau [material nuklir](https://id.wikipedia.org/w/index.php?title=Material_nuklir&action=edit&redlink=1).

Jumlah efek negatif kejahatan terorganisasi transnasional tidak pasti. Kejahatan terorganisasi transnasional dapat mengganggu demokrasi, menghambat [pasar bebas](https://id.wikipedia.org/wiki/Pasar_bebas), menguras aset negara, dan mencegah pembangunan masyarakat yang stabil. Atas alasan tersebut, kelompok penjahat nasional dan internasional dapat dikatakan mengancam keamanan semua negara. Korban jaringan kejahatan transnasional adalah pemerintah yang tidak stabil atau tidak cukup kuat untuk mencegahnya. Mereka melakukan aktivitas ilegal yang menjadi sumber pendanaan kelompok. Kejahatan terorganisasi transnasional mengganggu perdamaian dan kestabilan negara di seluruh dunia lewat [penyuapan](https://id.wikipedia.org/wiki/Penyuapan), kekerasan, atau teror.

Menurut direktur eksekutif United Nations Office on Drugs and Crime, kejahatan terorganisasi transnasional kurang dipahami dengan baik. Dalam laporan kejahatan terorganisasi transnasional berskala besar oleh PBB tahun 2010, ia menulis bahwa, "informasi mengenai pasar dan tren kejahatan transnasional sangat sedikit. Beberapa penelitian yang ada berfokus pada sepotong masalah, berdasarkan sektor atau negara, bukan gambaran besarnya. Tanpa perspektif global, kebijakan yang berdasar kuat tidak dapat dirumuskan." Menanggapi ancaman ini, sejumlah badan penegak hukum menyusun serangkaian pendekatan efektif untuk melawan kejahatan terorganisasi transnasional.

Louise I. Shelley, direktur [*Terrorism, Transnational Crime and Corruption Center*](https://id.wikipedia.org/w/index.php?title=Terrorism,_Transnational_Crime_and_Corruption_Center&action=edit&redlink=1)*di*[*George Mason University*](https://id.wikipedia.org/w/index.php?title=George_Mason_University&action=edit&redlink=1), mengatakan:

Kejahatan transnasional akan menjadi isu terpenting bagi para pengambil keputusan abad ke-21 - sama pentingnya seperti Perang Dingin pada abad ke-20 dan kolonialisme pada abad ke-19. Teroris dan kelompok kejahatan transnasional akan berkembang karena mereka sangat diuntungkan oleh globalisasi. Mereka memanfaatkan peningkatan arus perjalanan, perdagangan, pergerakan uang yang cepat, telekomunikasi dan sambungan komputer, dan sangat mampu untuk berkembang.

*(https://id.wikipedia.org/wiki/Kejahatan\_terorganisasi\_transnasional)*

* **Cyber Crime**

Kejahatan dengan menggunakan teknologi baru yaitu komputer/labtop.

Jenis dan pelanggaran cyber crime sangat beragam sebagai akibat dari penerapan teknologi. Cyber crime dapat berupa penyadapan dan penyalahgunaan informasi atau data yang berbentuk elektronik maupun yang ditransfer secara elektronik, pencurian data elektronik, pornografi, penyalahgunaan anak sebagai objek melawan hukun, penipuan memalui internet, perjudian diinternet, pengrusakan website, disamping pengrusakkan system melalui virus, Trojan horse, signal grounding dan lain lain.

**Pelaku cyber crime :**

Perlu kita ketahui pelaku *cyber crime* adalah mereka yang memiliki keahlian tinggi dalam ilmu computer, pelaku *cyber crime* umumnya menguasai algoritma dan pemrograman computer unutk membuat script/kode malware, mereka dapat menganalisa cara kerja system computer dan jaringan, dan mampu menemukan celah pasa system yang kemudian akan menggunakan kelemahan tersebut untuk dapat masuk sehingga tindakan kejahatan seperti pencurian data dapat berhasil dilakukan.

**Jenis-jenis Cyber Crime**

Ada beberapa jenis kejahatan pada cyber crime yang dapat kita golongkan berdasarkan aktivitas yang dilakukannya seperti dijelaskan berikut ini yang dirangkum dari berbagai sumber.

1. Unauthorized Aces

Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Contoh dari tindak kriminal ini adalah Probing dan port.

1. Illegal Contents

Merupakan kejahatan yang dilakukan dengan cara memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap sebagai melanggar hukum atau menggangu ketertiban pada masyarakat umum, contohnya adalah penyebaran pornografi atau berita yang tidak benar.

1. Penyebaran virus secara sengaja

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

1. Cyber Espionage, Sabotage, and Extortion

Cyber Espionage merupakan sebuah kejahatan dengan cara memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

1. Carding

Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.

1. Hacking dan Cracker

Istilah hacker biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

1. Cybersquatting and Typosquatting

Cybersquatting merupakan sebuah kejahatan yang dilakukan dengan cara mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain.

1. Cyber Terorism

Tindakan cybercrime termasuk cyber terorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer.

**Contoh kasus cyber crime di Indonesia**

1. **Pencurian dan penggunaan account Internet milik orang lain**

Salah satu kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan mereka yang “dicuri” dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, “pencurian” account cukup menangkap “userid” dan “password” saja. Hanya informasi yang dicuri. Sementara itu orang yang kecurian tidak merasakan hilangnya “benda” yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, penggunan dibebani biaya penggunaan acocunt tersebut. Kasus ini banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan account curian oleh dua Warnet di Bandung.

1. **Membajak situs web**

Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di Indonesia menunjukkan satu (1) situs web dibajak setiap harinya. Hukum apa yang dapat digunakan untuk menjerat cracker ini?

1. **Denial of Service (DoS) dan Distributed DoS (DDos) attack**

DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja.

1. **Kejahatan yang berhubungan dengan nama domain**

Nama domain (domain name) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah cybersquatting. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat “domain plesetan”, yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah typosquatting.

1. **IDCERT ( Indonesia Computer Emergency Response Team)**

Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya “sendmail worm” (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah Computer Emergency Response Team (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi *point of contact*bagi orang untuk melaporkan masalah kemanan. IDCERT merupakan CERT Indonesia .

1. **Sertifikasi perangkat security**

Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia. Di Korea hal ini ditangani oleh Korea Information Security Agency.

*(*[*https://yuliatwn.wordpress.com/2015/12/05/pengertian-jenis-jenis-dan-contoh-*](https://yuliatwn.wordpress.com/2015/12/05/pengertian-jenis-jenis-dan-contoh-)*kasus-cyber-crime/)*

* **Kejahatan Narkotika;**

Narkotikan yang awalnya dikhususkan untuk obat tetapi justru dipakai untuk konsumsi sehari-hari dan berakibat merugikan pemakai dan lingkungan. Dilakukan dalam beberapa bentuk, antara lain : memproduksi narkotika atau psikotropika secara tidak sah, mengedarkan narkotika atau psikotropika secara tidak sah, menyimpan atau memiliki narkotika secara tidak sah, dan mempergunakan narkotika atau psikotropika secara tidak sah.

**Kejahatan dilihat dari aspek motifnya menurut Seeli:**

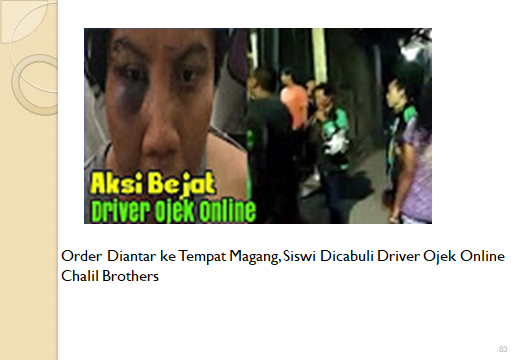
* Penjahat karena enggan bekerja
* Penjahat kekayaan uang (Pencurian uang)
* Penjahat agresif
* Penjahat nafsu seksual (Pemerkosaan)
* Penjahat karena krisis
* Penjahat yang bereaksi primitif
* Penjahat karena keyakinan (Contoh; Teroris)
* Penjahat karena kurang disiplin
* Penjahat bentuk campuran

**Kejahatan yang diatur dalam Hukum Pidana di Indonesia:**

* Kejahatan terhadap Orang, meliputi : Penganiayaan (Pasal ..KUHP), perkosaan, pembunuhan
* Kejahatan terhadap Harta Benda meliputi : Penipuan, pencurian, penggelapan.dll
* Kejahatan terhadap ketertiban umum meliputi : Pemabokan, perjudian. Dll
* Kejahatan terhadap negara, seperti Makar. (Pasal..KUHP
* Kejahatan Narkoba (UU Narkoba)
* Kejahatan Korupsi

**Beberapa tipologi kehjahatan dalam berita:**

* **Kejahatan dengan tipologi biasa**





**Kejahatan dengan tipologi *White Collar Crime***



****

**DAFTAR PUSTAKA**

Edwin H. Sutherland, Principles of Criminologi, diterjemahkan oleh Nomon Martasaputra, SH., Alumni 1969.

Yesmil Anwar dan Adang, Kriminologi, PT. Refika Aditama, 2013.

I.S. Susanto, Kriminologi, Genta Publishing, 2011.

I.S. Susanto, Statistik Krimina Sebagai Konstruksi Sosial, Penyusunan, Penggunaan dan Penyebarannya, Suatu Studi Kriminologi, Genta Publishing, 2011.

Romli Atmasasmita, Teori dan Kapita Selekta Kriminologi, Refika Aditama, 2013.

M. Ali Zaidan, Kebijakan Kriminal, Sinar Grafika, 2016

B. Simanjuntak, Pengantar Kriminologi dan Patologi Sosial,

*(*[*https://yuliatwn.wordpress.com/2015/12/05/pengertian-jenis-jenis-dan-contoh-kasus-cyber-crime/*](https://yuliatwn.wordpress.com/2015/12/05/pengertian-jenis-jenis-dan-contoh-kasus-cyber-crime/)*)*

*(https://medium.com/@dwitaks/kejahatan-kerah-putih-white-collar-crime-di-asia-5199c723601e)*