PENTINGNYA PEMAHAMAN KEJAHATAN CYBER DAN PENEGAKAN HUKUM DALAM STRATEGI RESPONS YANG EFEKTIF

(in English)

THE IMPORTANCE OF UNDERSTANDING CYBER CRIME AND LAW ENFORCEMENT IN EFFECTIVE RESPONSE STRATEGIES

Muhamad Arif Ramdani Budiman, Fachri Rajib Khairi Hakim, Nurhan Ahmad, Zikrulloh Apandi, Muhamad Rafi
Fakultas Hukum Universitas Nusa Putra, Sukabumi
muhamadariframdanibudiman18@gmail.com, fachri.rajib_hk23@nusaputra.ac.id,
nurhan.ahmad_hk23@nusaputra.ac.id, apandizikrulloh@gmail.com, muhamad.rafi_hk23@nusaputra.ac.id

ABSTRACT

This legal writing is motivated by the fact that information technology plays an important role in human life both now and in the future. The implications of the growth of information technology bring people to an increasingly open pattern of behavior. With the presence of the internet, it makes human life around the world easier. Because the internet can penetrate the boundaries between countries and accelerate the spread and exchange of knowledge both among scientists or scholars around the world. However, behind the ease of using the internet, there is a dark side that worries its users, namely in terms of security. The security of internet-based computer systems needs to be considered. Because internet networks that are public and global are very vulnerable to various forms of cybercrime or cyber crime. Cracker crime Cracker is a perpetrator or person who carries out cracking activities on the internet. The consequences of these crimes are very detrimental. Among them is that it can damage the network, sites cannot be opened, deleted data and others. Because the modus operandi of this cracker is different from other conventional crimes. And the most distinguishing is the locus delicti or place of crime. After knowing the modus operandi of crackers, it will be easy to be able to handle cracker cases.

Keyword: *Cyber Crime, Cracking Internet, Scamming*

ABSTRAK

Penulisan hukum ini dilatarbelakangi bahwa teknologi informasi memegang peranan penting dalam kehidupan manusia baik di masa kini maupun masa yang akan datang. Implikasi dari pertumbuhan teknologi informasi membawa masyarakat kepada pola perilaku yang semakin terbuka. Dengan kehadiran internet, maka membuat kehidupan manusia di seluruh dunia menjadi lebih mudah. Karena internet dapat menembus batas-batas antarnegara dan mempercepat penyebaran dan pertukaran ilmu baik dikalangan ilmuwan atau cendekiawan di seluruh dunia. Hanya saja, dibalik kemudahan penggunaan internet, terdapat sisi gelap yang merisaukan penggunanya, yaitu dari segi keamanannya. Keamanan sistem komputer berbasis internet perlu diperhatikan. Karena jaringan internet yang bersifat publik dan global sangat rentan dari berbagai bentuk kejahatan dunia maya atau *cybercrime.* Terutama kejahatan *cracker. Cracker* adalah pelaku atau orang yang melakukan aktivitas *cracking* di internet. Akibat dari kejahatan tersebut sangat merugikan. Diantaranya adalah dapat merusak jaringan, situs tidak dapat dibuka, terhapusnya data-data dan lain-lain. Karena modus operandi cracker ini berbeda dengan kejahatan konvensional lainnya. Dan yang paling membedakan adalah locus delicti nya atau tempat kejahatan perkara. Setelah mengetahui modus operasi *cracker* ,maka akan dengan mudah untuk dapat menangani kasus *cracker.*

Kata Kunci: Kejahatan Dunia Maya, Peretasan Internet, Penipuan

PENDAHULUAN

Berkaitan dengan semakin pesatnya perkembangan ilmu pengetahuan dan teknologi informasi (IPTEK) saat ini, berpengaruh besar dalam perubahan perilaku dan hukum dalam masyarakat. Memajukan kehidupan masyarakat modern terhadap teknologi merupakan salah satu kunci keberhasilan dan kemajuan dalam pembangunan. Kemajuan teknologi informasi termasuk telekomunikasi tidak hanya terjadi pada negara maju, namun juga terhadap negara berkembang. Indonesia adalah salah satu negara yang perkembangan teknologinya saat ini sedang berkembang dengan pesat termasuk dalam di bidang ilmu pengetahuan, sosial, ekonomi, dan budaya. Pemanfaatan teknologi tersebut telah mendorong pertumbuhan bisnis yang pesat, karena berbagai informasi telah dapat disajikan dengan canggih dan mudah diperoleh, dan melalui hubungan jarak jauh dengan memanfaatkan teknologi telekomunikasi dapat digunakan untuk bahan melakukan langkah bisnis selanjutnya. Umumnya suatu masyarakat yang mengalami perubahan akibat kemajuan teknologi, banyak melahirkan masalah-masalah sosial. Hal itu terjadi karena kondisi masyarakat itu sendiri yang belum siap menerima perubahan atau dapat pula karena nilai-nilai masyarakat yang telah berubah dalam menilai kondisi. Lama sebagai kondisi yang tidak lagi dapat diterima. Salah satu hasil kemajuan teknologi yaitu penggunaan internet. Peran internet sangat penting bagi masyarakat. Melalui internet kita dapat mengetahui berbagai hal, mulai dari media sosial, aplikasi, berita, gaya hidup, bahkan kita dapat melakukan kegiatan apapun.

Perkembangan teknologi, dapat menimbulkan dampak positif dan dampak negatif. Salah satu dampak negatif yang ditimbulkan karena perkembangan teknologi yaitu munculnya ancaman kejahatan-kejahatan yang modern. Kejahatan terus berkembang seiring dengan perkembangan peradaban manusia, dengan kualitas dan kuantitasnya kompleks dengan variasi modus operandinya. Melalui media internet beberapa jenis tindak pidana semakin mudah untuk dilakukan seperti, tindak pidana pencemaran nama baik, pornografi, perjudian, pembobolan rekening, kerusakan jaringan *cyber (hacking),* penyerangan melalui virus *(virus attack)* dan sebagainya.[1]

Kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi dan telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet, atau dalam istilah asing sering disebut *cybercrime*. Namun dalam pandangan lain *cybercrime* ini bisa dikatakan sebagai dampak positif dari perkembangan teknologi saat ini, yaitu seseorang memanfaatkan perkembangan teknologi. Akan tetapi, hal ini dimanfaatkan oleh oknum tertentu untuk melakukan kejahatan hingga *cybercrime* ini dikatakan sebagai tindak pidana. Sedangkan tindak pidana yang diketahui oleh masyarakat adalah tindakan yang merugikan sebagian pihak dan nampak terlihat tindakannya tersebut, seperti pencurian, pembunuhan. Lalu, mengapa *cybercrime* ini bisa dikatakan sebagai tindak pidana, apa yang telah diambil oleh cybercrime dan apa yang telah dibunuh oleh *cybercrime* sehingga hal tersebut dikatakan sebagai tindak pidana. Dan bagaimana penegakkan hukum terhadap kasus *cybercrime*. Kasus yang sedang heboh saat ini adalah penipuan investasi bodong. Pada awalnya investasi bodong adalah kegiatan yang menawarkan penggandaan uang melalui sistem elektronik, transaksi dilakukan dengan sistem pembayaran yang telah ditentukan. Setelah itu, pelaku seolah-olah memproses uang tersebut dengan waktu tertentu dan telah disepakati bersama, sesudah ada hasil dari investasi sebelumnya pelaku meminta kembali uang untuk penebusan investasi yang diproses di awal tadi. Dalam hal penipuan, KUHAP mengatur tidak hanya memuat ketentuan tentang hukum acara pidana, tetapi juga mencakup hak dan kewajiban para pihak dalam hukum acara pidana. KUHAP juga mengatur tentang penyelidikan dan penyidikan. Penyidikan pendahuluan dimulai setelah kejahatan dilakukan, sehingga perbuatannya diatur oleh hukum yang bersifat menindas (pidana). Fokus penyelidikan pendahuluan adalah pencarian dan pengumpulan bukti-bukti untuk mengidentifikasi tindak pidana yang muncul serta menemukan dan mengungkap pelakunya. Dalam lingkungan hukum, polisi berfungsi sebagai penyidik. Dalam tugasnya, polisi mencari informasi dari berbagai sumber dan saksi. Penyidikan pidana adalah tindakan penyidik menurut tata cara yang diberikan undang-undang, yang tujuannya mencari dan mengumpulkan bukti-bukti tentang suatu tindak pidana yang terjadi guna menemukan tersangka. Dalam penyelidikan dan penyidikan serta dalam penyidikan tindak pidana penipuan investasi yang berkedok Koin Emas, POLRI selaku penyidik umum proses penyidikan melakukan penyidikan, mengumpulkan keterangan terkait fakta-fakta tertentu untuk membuktikan siapa yang melakukan tindak pidana tersebut. dan menyajikan bukti kejahatan untuk menjelaskan masalah tersebut dengan mengumpulkan bukti yang tersedia terkait dengan tindak pidana Bodong/Investasi Koin Emas.[2]

[1] Tubagus Heru Dharma Wijaya, Nanda Sahputra Umara, "Cybercrime", No. 2 (2022), hlm. 373.

[2] I Kadek Moleh, A.A Gde Putra Arjawa, I Gusti Ngurah Aristiawan, "Proses Penyidikan Tindak Pidana Investasi Bodong (Gold Coin) di Ditreskrimsus Polda Bali", No. 2 (2023), hlm. 64.

RUMUSAN MASALAH

a. Bagaimana bentuk tindak pidana kejahatan cybercrime di indonesia?
b. Implementasi Penegakan hukum terhadap pelaku tindak pidana kejahatan cybercrime?

METODE PENELITIAN

Tipe penelitian yang digunakan untuk penelitian ini merupakan "tipe penelitian hukum doktrinal" ataupun "penelitian hukum normatif (normative legal research)". Penelitian normatif adalah penelitian hukum kepustakaan yang di Negara-negara yang sudah lazim disebut "Legal Research" atau "Legal Research Instruction," dengan Pendekatan Perundang-undangan (Statute Approach), Pendekatan Kasus (Case Approach), Pendekatan Konseptual, Pendekatan Analitis (Analytical Approach), Pendekatan Teori (Theoretical Approach). Jenis dan sumber bahan hukum yaitu bahan hukum primer, merupakan bahan hukum yang bersumber pada Kitab Suci maupun bahan hukum yang bersumber dari berbagai peraturan perundang-undangan, yakni Undang-Undang Dasar Negara Republik Indonesia tahun 1945, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016 tentang perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi dan pengaturan hukum terkait penipuan online dapat diakomodasi melalui pasal 378 KUHP.
Elektronik, bahan hukum sekunder, merupakan berbagai referensi ataupun karya-karya ilmiah bidang hukum, berupa buku hukum, artikel hukum, jurnal hukum, naskah pidato pengukuhan guru besar bidang hukum, naskah orasi ilmiah dibidang hukum dan naskah-naskah akademik bidang hukum, naskah hukum hasil lokakarya dan sebagainya, bahan hukum tersier, merupakan bahan hukum yang sifatnya pelengkap, yakni melengkapi dua bahan yang lain yakni bahan hukum primer dan bahan hukum sekunder. Bahan hukum tersier misalnya kamus-kamus umum, kamus hukum maupun terminologi hukum yang menjadi dasar untuk seorang peneliti di bidang hukum dalam menelusuri makna dan arti sebuah kata atau kalimat yang berhubungan dengan bidang hukum, termasuk juga ensiklopedia. Teknik pengumpulan bahan hukum yang digunakan pada penelitian ini berdasarkan pengamatan maupun penelusuran cermat terhadap berbagai bahan hukum sebagaimana disebutkan di atas, yakni penelusuran bahan hukum primer, bahan hukum sekunder maupun bahan hukum tersier. Analisis bahan hukum yang digunakan dalam penelitian ini merupakan jenis analisis kualitatif, analisis kualitatif kebanyakan dipergunakan pada tipe penelitian hukum dengan karakteristik penelitian hukum normatif yang datanya berasal dari kepustakaan, berupa bahan-bahan hukum, seperti bahan hukum primer, bahan hukum sekunder maupun bahan hukum tersier. Mengenai analisis yuridis normatif pada esensinya memfokuskan pada metode deduktif untuk pegangan utama, dan metode induktif sebagai tata kerja penunjang. Analisis normatif utamanya menggunakan bahan-bahan kepustakaan sebagai sumber data penelitiannya.

PEMBAHASAN DAN ANALISIS

Terbentuknya Jaringan Komputer di Tengah Masyarakat Modus operandi cracker ini berbeda dengan tindak kejahatan konvensional. Hal yang paling mencolok dari perbedaan tersebut antara lain adalah terletak pada locus delicti atau tempat kejahatan perkara, karena dalam kejahatan ini yang diserang adalah jaringan komputer atau internet. Sehingga dikatakan sulit karena memang sulitnya melokalisir jaringan internet, hal ini terkait dengan jaringan-jaringan yang ada pada komputer. Pada tahun 1977, ada dua orang anak muda kreatif, Steve Jobs dan Steve Wozniak dari Lembah Silicon Valley, California. Mereka memperkenalkan konsep baru, sebuah personal computer, yang diberi nama Apple Komputer Generasi I. Dengan harapan satu orang satu komputer, ternyata konsep ini disambut hangat rakyat Amerika. Oleh karena itu kemudian komputer tersebut diberi nama personal computer (PC) atau komputer rumah tangga atau komputer pribadi. Ternyata prinsip-prinsip ini diadopsi oleh perusahaan-perusahaan lain. Perusahaan IBM dan Hewlett Packard yang dulunya bergerak di bidang komputer mini dan mainframe ikut terjun menambah ramai bisnis personal komputer atau PC hingga seperti yang terjadi saat ini. Dalam perkembangannya kehadiran dari personal komputer atau PC berkembang dengan sangat pesat. Industri perangkat keras atau hardware komputer "membludak" dan menyebabkan harganya semakin murah, sehingga masyarakat umum semakin banyak yang mampu memiliki komputer di masing-masing rumah. Komputer pun pada akhirnya bukan lagi dapat dimonopoli orang-orang kaya atau perusahaan besar atau kantor-kantor pemerintah, tetapi sudah terjangkau oleh sebuah rumah tangga yang sederhana. Bahkan, memiliki sebuah laptop atau notebook seolah-olah sudah menjadi hal yang biasa. Banyak yang bisa kita lihat di tempat-tempat umum adanya orang orang yang tengah asyik dengan laptopnya. Orang yang menggunakan laptop tidak hanya bisa dilihat di kampus-kampus. Di bandara, rumah sakit, terminal, stasiun, pasar, mall dan sebagainya juga sudah terbiasa dijumpai orang-orang yang menggunakan laptop. Kejahatan Meretas Komputer Kemudian terbentuklah sebuah jaringan komputer yang dapat tersambung antara yang satu dengan yang lain dalam posisi yang sama kuat. Jaringan internet itu menimbulkan kenyamanan bagi para operator komputer, karena memudahkan cara kerja pemakai komputer. Jaringan komputer yang saling terhubung

melalui satelit ini kemudian dikenal dengan jaringan internet. Dengan adanya sistem jaringan internet pengakses dapat saling tukar pengetahuan, saling tukar informasi atau saling tukar data-data, antara komputer yang satu dengan komputer yang lain, dapat dilakukan dengan kecepatan yang cukup tinggi, tidak membutuhkan tempat yang besar, cukup dilakukan dari ruangan kecil yang menghemat biaya. Dalam perkembangan, sebuah jaringan komputer atau jaringan internet merupakan suatu kebutuhan setiap orang, tiap perusahaan, dan setiap pemerintah. Pekerjaan yang biasanya dapat dilakukan berhari hari bahkan berminggu-minggu, dengan hadirnya komputer jaringan atau internet biaya dapat dipangkas sedemikian rupa. Perasaan nyaman karena semua orang dapat bekerja lebih efektif dan efisien dengan sarana komputer dan internet. Hanya saja dalam perkembangannya kemudian jaringan itu digunakan sebagai sarana yang negatif, atau metode itu dapat dimanfaatkan oleh penjahat komputer untuk melihat, mengubah, atau merusak jaringan milik orang lain, seperti yang dilakukan oleh para cracker.

Kejahatan yang dilakukan oleh cracker adalah produk manusia modern, yang tidak memerlukan kekerasan fisik, namun dapat dikendalikan melalui suatu ruangan tertentu. Modalnya juga tidak terlalu besar, namun dapat menghasilkan uang yang cukup banyak dari hasil kejahatan tersebut.

Di Indonesia, kejahatan yang menggunakan sarana komputer sebenarnya sudah lama terjadi, namun pada saat ini sangat sulit dideteksi karena berbagai hal, baik lihat dari sumber daya manusianya, maupun dari sisi hukum yang memayunginya. Dari tahun ke tahun usaha untuk melakukan kejahatan ini terus meningkat, seiring dengan kemajuan teknologi dan kemajuan berfikir manusia. Di sisi lain, usaha-usaha untuk melakukan penegakan hukum masih belum ada perkembangannya. Akibat kejahatan yang dilakukan cracker ini, nama Indonesia menjadi kurang baik karena masuk dalam daftar hitam di kalangan penyedia layanan-layanan pembayaran lewat internet atau online payment. Hal ini sungguh memprihatinkan karena pada masa yang sulit ini akibat krisis ekonomi, Indonesia sebenarnya tengah memulihkan namanya di forum perdagangan internasional. Ketika sudah mulai diperhitungkan dalam iklim investasi dunia karena berkat berbagai kemudahan dalam infrastruktur perdagangan global pembayaran atau transaksi melalui layanan internet, ternyata banyak tangan-tangan jahil yang berlaku tidak baik dengan melakukan kejahatan menggunakan internet sebagai sarananya. Baik buruknya output atau hasil akhir dari suatu pemanfaatan komputer tergantung operatornya. Peran operator sangat menentukan apakah operasi yang dilakukan oleh operator merugikan banyak orang atau tidak, menyangkut perbuatan pidana atau tidak. Untuk memperjelas hal tersebut dikemukakan pendapat para ahli sebagai berikut. Suatu perbuatan bisa dijadikan perbuatan pidana atau dikriminalisasikan menurut TB. Ronny R. Nitibaskara, karena alasan: Perbuatan itu merugikan masyarakat; Sudah berulang-ulang dilakukan; Ada reaksi sosial atas perbuatan itu; Ada unsur bukti. Berdasarkan keempat parameter ini, maka tidak serta merta setiap perbuatan yang merugikan dapat dirumuskan secara formal sebagai perbuatan pidana. Oleh karena itu, di dalam dunia cyber perlu dipilah dengan seksama, mana saja perbuatan-perbuatan yang layak dikategorikan sebagai kejahatan pidana seperti cracker. Kejahatan yang dilakukan oleh cracker ini pada awalnya sulit dilacak, karena selalu ada suatu metode untuk menghilangkan jejak dengan logika yang sudah dikuasai oleh operatornya. Ada beberapa hal yang menyebabkan suatu kejahatan ini sulit dilacak antara lain: Di dalam sebuah perusahaan, data-data komputer biasanya ditangani oleh Electronic Data Processing (EDP), dimana disitu ada auditor; Masih sedikitnya pegawai-pegawai selaku operator komputer yang mengetahui cara kerja komputer secara rinci; Para pelaku kejahatan komputer adalah orang-orang yang pada umumnya cerdas dan mempunyai perasaan keingintahuan yang besar, fanatik akan teknologi komputer; Buku-buku tentang kejahatan komputer tidak banyak; Kejahatan komputer itu terselubung dan terorganisir. Tidaklah mudah bagi seseorang untuk menyelidiki kegiatan kejahatan komputer; Mudah dilakukan, resiko untuk ketahuan kecil dan tidak diperlukan peralatan yang super modern; Jarang sekali ada seminar-seminar atau mata kuliah tentang pencegahan terhadap kejahatan komputer; Terlalu percaya pada komputer; Kurangnya perhatian dari masyarakat. Atas dasar hal-hal tersebut, lahirlah kesulitan para penegak hukum untuk menemukan kejahatan yang menggunakan sarana komputer seperti yang dilakukan oleh cracker atas aktivitas crackingnya di internet. Disamping sulitnya melakukan pelacakan karena faktor di atas, juga karena faktor sumber daya manusianya. Untuk melakukan penyidikan terhadap kejahatan cracker ini harus mempunyai keahlian di bidang komputer dan jaringannya dan setelah itu perlu peranan ahli komputer yang secara teknis menerangkan kepada penyidik. Modus Operandi Cracker Adapun modus operandi yang dilakukan oleh para cracker dalam Pasal 30 UU ITE biasanya disebut Unauthorized Access to Computer System and Service, yaitu kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik resmi sistem jaringan komputer yang dimasukinya. Biasanya seorang pelaku kejahatan atau cracker melakukannya dengan maksud sabotase ataupun melakukan pencurian informasi penting dan rahasia. Adapun Langkah-langkah yang dilakukan oleh cracker kurang lebih sama, sedangkan yang berbeda adalah dampak yang ditimbulkan. Suatu cracking bisa terjadi jika ada suatu akses ke dalam

suatu sistem yang dituju atau dimasuki mengalami kerusakan, dan kerusakan tersebut bisa membuat sistem tidak berfungsi, dan harus dilakukan pembenahan secara besar-besaran terhadap suatu sistem komputer yang telah rusak. Adapun proses penyusupan dalam dunia cracker dibedakan menjadi beberapa tahapan yaitu sebagai berikut: Pertama, Footprinting dan/atau Pencarian Data: Cracker baru mencari sistem yang dapat disusupi. Footprinting adalah merupakan kegiatan pencarian data berupa: Menentukan ruang lingkup atau scope aktivitas atau serangan; Network enumeration atau menyeleksi jaringan; Interogasi jaringan; Mengintai jaringan. Semua kegiatan ini dapat dilakukan dengan alat atau tools dan merupakan informasi yang tersedia bebas di internet. Kegiatan footprinting ini dapat diibaratkan mencari informasi yang tersedia umum melalui buku telepon. Kedua, yaitu Scanning atau Pemilihan Sasaran: Lebih bersifat aktif terhadap sistem sasaran. Disini diibaratkan cracker sudah mulai mengetuk-ngetuk dinding sistem sasaran untuk mencari apakah ada kelemahannya. Kegiatan scanning dengan demikian dari segi jaringan sangat berisik dan mudah dikenali oleh sistem yang dijadikan sasaran, kecuali dengan menggunakan stealth scanning. Scanning tool yang paling legendaris adalah nmap (yang kini tersedia pula untuk Windows 9x/ME maupun DOS), selain SuperScan dan Ultrascan yang juga digunakan pada sistem Windows. Untuk melindungi diri dari kegiatan scanning adalah memasang Firewall misalnya Zone Alarm, atau bila ada keseluruhan network, dengan menggunakan aplikasi Intrusion Detection System(IDS) misalnya Snort. Ketiga, Enumerasi atau Pencarian Data Mengenai Sasaran: Sudah bersifat sangat intrusif (mengganggu) terhadap suatu sistem. Disini para penyusup dapat mencari account name yang absah, password, serta share resources yang ada. Pada tahap ini, khusus untuk sistem Windows, terdapat port 139 (NetBIOS session service) yang terbuka untuk resource sharing antar pemakai dalam jaringan. beberapa orang mungkin berpikir bahwa harddisk yang di-share itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannya tidak demikian. NetBIOS session service dapat dilihat oleh siapa pun yang terhubung ke Internet di seluruh dunia. Tools seperti legion, SMB Scanner, atau Shares Finder membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka resource share tanpa pemberian password). Keempat, Gaining Access atau dikatakan Akses Ilegal telah Ditetapkan: adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai user biasa. Ini adalah kelanjutan dari kegiatan enumerasi, sehingga biasanya disini seorang penyerang sudah mempunyai paling tidak user account yang absah, dan tinggal mencari passwordnya aja. Bila resource share-nya diproteksi dengan suatu password, maka password ini dapat saja ditebak (karena banyak yang menggunakan password sederhana dalam melindungi komputernya). Menebaknya dapat secara otomatis melalui dictionary attack (mencobakan kata-kata dari kamus sebagai suatu password) atau brute-force attack (mencobakan kombinasi semua karakter sebagai password). Dari sini penyerang mungkin akan berhasil memperoleh log-on sebagai user yang absah. Kelima, Escalating Privilege (Menaikkan atau Mengamankan suatu Posisi): Mengasumsikan bahwa penyerang sudah mendapatkan log-on access pada sistem sebagai user biasa. Penyerang kini berusaha naik kelas menjadi admin (pada sistem windows) atau menjadi root (pada sistem Unix atau Linux). Teknik yang digunakan sudah tidak lagi dictionary attack atau brute-force attack yang memakan waktu itu, melainkan mencuri password file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem Windows 9x/ME password disimpan dalam file PWL sedangkan pada Windows NT/2000 dalam file.SAM. Bahaya pada tahap ini bukan hanya dari penyerang di luar sistem melainkan lebih besar Sa'diyah, Modus Operandi Tindak Pidana Cracker lagi bahayanya adalah orang dalam, yaitu user absah dalam jaringan itu sendiri yang berusaha naik kelas menjadi admin atau root. Keenam, Pilfering atau Suatu Proses Pencurian: Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di registry, config file, dan user data. Ketujuh, Covering Tracks atau Menutup Jejak: Begitu kontrol penuh terhadap sistem yang diperoleh, maka menutup jejak menjadi suatu prioritas. Meliputi membersihkan network log dan penggunaan hide tools seperti macam-macam rootkit dan file streaming.Kedelapan, Creating Backdoors atau Membuat Jalan Pintas: Pintu belakang diciptakan pada berbagai bagian dari suatu sistem untuk memudahkan masuk kembali. Pada tahap keenam, ketujuh dan kedelapan, penyerang sudah berada dan menguasai suatu sistem dan kini berusaha untuk mencari informasi lanjutan atau pilfering, menutupi jejak penyusupannya atau covering tracks, dan menyiapkan pintu belakang atau creating backdoor agar lain kali dapat dengan mudah masuk lagi ke dalam sistem. Adanya trojan pada suatu sistem berarti suatu sistem dapat dengan mudah dimasuki penyerang tanpa harus bersusah payah melalui tahapan-tahapan di atas, hanya karena kecerobohan pemakai komputer itu sendiri. Kesembilan, Denial of Service atau Melumpuhkan Sistem: Bukanlah tahapan terakhir, melainkan kalau penyerang sudah frustasi tidak dapat masuk ke dalam sistem yang kuat pertahanannya, maka yang dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu crash atau kacau. Denial of service attack sangat sulit dicegah, sebab memakan habis bandwidth yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP

yang bersangkutan. Para script kiddies yang pengetahuan cracking-nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

A. Kejahatan komputer

Kejahatan meretas komputer merupakan suatu seni dalam menembus sistem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana cara berfungsinya. Kejahatan mengakses komputer tanpa izin adalah ilegal karena masuk dan membaca data seseorang tanpa izin dengan cara sembunyi-sembunyi sama saja dengan pissing people off orang, sehingga para hacker (orang yang melakukan peretasan pada komputer) selalu menyembunyikan identitas mereka. Walaupun ilegal namun hacker tidak seluruhnya jahat, hacker yang baik motifnya hanya untuk mencari tantangan dan kesenangan saja, membuktikan dirinya mampu menembus sistem. Hacker seperti itu disebut real hacker atau hacker sejati. Peraturan perundang-undangan di Indonesia tidak mengenal istilah hacking (meretas). Secara harfiah hacking berasal dari kata ”hack” dari bahasa Inggris yang berarti mencincang atau membacok. Namun dalam kejahatan internet hacking (meretas) dapat diartikan sebagai penyusupan atau perusakan suatu sistem komputer. Dalam Pasal 30 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Pasal 30 ayat (3), dapat disimpulkan bahwa meretas komputer merupakan perbuatan setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.[3]

A. Karakteristik Cybercrime

Ada beberapa jenis kejahatan pada cybercrime yang bisa diklasifikasikan berdasarkan aktivitas seperti:

- **Akses tidak sah**

Ini adalah kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan pemilik sistem jaringan komputer yang dimilikinya. Contoh kejahatan ini adalah Probing dan port.

- **Konten Ilegal**

Ini adalah kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang hal yang tidak benar, tidak etis, dan dapat dianggap sebagai tindakan hukum yang melanggar hukum atau mengganggu, misalnya penyebaran pornografi atau berita yang tidak benar.

Penyebaran Virus Penyebaran virus umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terpapar virus tidak menyadari hal ini. Virus ini kemudian dikirim ke tempat lain via email.

- **Cyber Spionase, Sabotase, dan Pemerasan**
  Cyber Spionase

adalah kejahatan dengan cara memanfaatkan jaringan internet untuk melakukan spionase pihak lain, dengan memasukkan sistem jaringan komputer target. Sabotase dan Pemerasan adalah jenis kejahatan yang dilakukan dengan melakukan gangguan, penghancuran atau penghancuran data, program komputer atau sistem jaringan komputer yang terhubung ke internet.

- **Carding Carding**

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

- **Hacking dan Cracking**

Istilah hacker biasanya mengacu pada seseorang yang memiliki minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kemampuannya.

Aktivitas cracking di internet memiliki cakupan yang sangat luas, mulai dari pembajakan akun orang lain, pembajakan situs web, penyelidikan, penyebaran virus, hingga penonaktifan target. Tindakan terakhir disebut DoS (Denial Of Service). Serangan DoS adalah serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak bisa memberikan layanan.

- **Cybersquatting dan Typosquatting**
  Cybersquatting

adalah kejahatan yang dilakukan dengan mendaftarkan nama domain perusahaan perusahaan lain dan kemudian mencoba menjualnya ke perusahaan dengan harga yang lebih tinggi. Typosquatting adalah kejahatan dengan menciptakan domain palsu yang merupakan domain yang mirip dengan nama domain orang lain.

- **Cyber Terrorism**

Tindakan cybercrime termasuk terorisme cyber jika mengancam pemerintah atau warga negara, termasuk melakukan cracking ke lokasi pemerintah atau militer.[4]

B. Konsekuensi Pelaku Cybercrime

Implementasi penegakan hukum Cyber crime tersendiri di Indonesia diatur dalam Undang-Undang Transaksi Elektronik Nomor 8 Tahun 2011 sebagaimana telah diubah menjadi Undang-Undang Nomor 19 Tahun 2016, ("UU ITE") khususnya pada pasal 27 sampai 30 mengenai perbuatan yang dilarang. Lebih lanjut, aturan tentang hacking diatur dalam pasal 30 ayat (1), (2) dan (3) mengatakan bahwa:

1. Dengan sengaja tanpa hak dan tanpa hak atau melawan hukum mengakses dan/atau sistem elektronik orang lain dengan cara apapun

[3] Nur Khalimatus Sa’diyah,”Modus operandi tindak pidana cracker”, No. 2 (2012), hlm. 81.

[4] Andysah Putera Utama Siahaan,”Pelanggaran cybercrime dan kekuatan yurisdiksi di indonesia”, No. 1 (2018), hlm. 7.

2. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem orang lain dengan cara apapun untuk tujuan memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
3. Dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan tujuan melanggar menerobos, melampaui, menjebol sistem pengaman Lebih lanjut sanksi bagi yang melanggar ketentuan pasal 30 UU ITE diatur di dalam pasal 46 UU ITE berupa:
1. Ayat (1): dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
2. ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
3. ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).[5]

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, kesimpulan yang diperoleh adalah sebagai berikut:
1. Terkait bagaimana bentuk tindak pidana dalam Cyber Crime dalam hukum positif di indonesia, diperoleh kesimpulan sebagai berikut:
Pasal 46 UU ITE Menjelaskan tentang sanksi Tindakan Cyber Crime :
1. Ayat (1): dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
2. ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
3. ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).
2. Terkait juga dengan Implementasi Penegakan Hukum Terhadap Pelaku tindak pidana Cyber Crime : Perkembangan teknologi informasi tidak hanya memberikan manfaat tetapi juga membawa dampak negatif yang menyertainya. Dalam tindak pidana cyber crime ini tidak memilah siapa korbannya, tidak hanya masyarakat tetapi juga pada aparatur pemerintahan.

SARAN

Penguatan Hukum dan Penegakan Hukum:
Perlu adanya penguatan dalam perundang-undangan terkait kejahatan komputer, termasuk penambahan sanksi yang lebih tegas.
Pentingnya penegakan hukum yang efektif dan efisien dalam menangani kejahatan komputer agar dapat memberikan efek jera dan melindungi masyarakat.
Peningkatan Kesadaran dan Pendidikan:
Kampanye edukasi kepada masyarakat tentang risiko kejahatan komputer dan langkah-langkah pencegahannya.
Peningkatan kurikulum pendidikan untuk mencakup literasi digital dan keamanan cyber.
Kerja Sama Internasional:
Perlu adanya kerja sama antarnegara dalam penanganan kejahatan komputer, mengingat sifatnya yang lintas batas.
Pertukaran informasi dan koordinasi antar lembaga penegak hukum dari berbagai negara untuk memberantas jaringan kejahatan komputer.
Pengembangan Keamanan Teknologi:
Inovasi terus-menerus dalam pengembangan sistem keamanan teknologi untuk mengurangi celah yang dapat dieksploitasi oleh para cracker.
Dorongan bagi perusahaan dan individu untuk menggunakan sistem keamanan yang lebih canggih.
Penelitian dan Pengembangan:
Dukungan untuk penelitian dan pengembangan dalam bidang keamanan cyber guna menemukan solusi baru dan meningkatkan ketahanan sistem komputer.
Pelibatan Masyarakat:
Masyarakat perlu lebih aktif melaporkan kejahatan komputer yang mereka alami atau saksikan.
Pembentukan kelompok keamanan siber masyarakat untuk saling bertukar informasi dan pengalaman.
Perlindungan Privasi:
Penekanan pada perlindungan data pribadi agar tidak mudah diakses oleh pihak yang tidak berwenang.
Regulasi yang lebih ketat terkait dengan pengelolaan data oleh perusahaan dan organisasi.

DAFTAR KEPUSTAKAAN

Andysah Putera Utama Siahaan. “PELANGGARAN CYBERCRIME DAN KEKUATAN YURISDIKSI DI INDONESIA.” vol. VOL.5 NO.1, 2018. Accessed Selasa Desember 2023.

Duwi Handoko. “TINDAK PIDANA TANPA KORBAN DI INDONESIA PENGATURAN DAN PROBLEMATIKANYA.” vol. Vol. XII, No. 3, no. April, 2018. Accessed Kamis Desember 2023.

H Sofwan Jannah &M. Naufal. “PENEGAKAN HUKUM CYBER CRIME DITINJAU DARI HUKUM POSITIF DAN HUKUM ISLAM.” vol. VOL. XII, NO 1, no. Februari, 2012. Accessed Rabu Desember 2023.

I Kadek Moleh, et al. *Proses Penyidikan Tindak Pidana Investasi Bodong (Gold Coin) di Ditreskrimsus Polda Bali*, vol. Vol. 1, No. 2, no. Juli, 2023. Accessed Rabu Desember 2023.

Nur Khalimates Sa'diyah. “MODUS OPERANDI TINDAK PIDANA CRACKER MENURUT UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK.” vol. Volume

[5] H Sofwan Jannah &M. Naufal, “Penegakan hukum cybercrime dari hukum positif dan hukum islam” No. 1 (2012), hlm. 74.

XVII No. 2, no. Mei, 2012. Accessed Rabu Desember 2023.

Tubagus Heru Dharma Wijaya, and Nanda Sahputra Umara. “PENERAPAN SANKSI SOSIAL SEBAGAI ALTERNATIF PEMIDANAAN TERHADAP PELAKU TINDAK PIDANA KEJAHATAN SIBER (CYBER CRIME).” vol. VOL 5 NO. 2, 2022. Accessed Selasa Desember 2023.