MODUL
CYBER CRIME

Devie Rahmawati; Giri Lumakto; Rizki Ameliah;
Mila Viendyasari; Rangga Adi Negara;
Aisyah Adinda; Syavia Bachna

Penulis:

Devie Rahmawati; Giri Lumakto; Rizki Ameliah; Mila Viendyasari; Rangga Adi Negara; Aisyah Adinda; Syavia Bachna

MODUL
CYBER CRIME

Penerbit :

Program Studi Hubungan Masyarakat Program Vokasi

Universitas Indonesia

MODUL
CYBER CRIME

Dewan Pembina:

Prof. Dr. drg. Indang Trihandini., M.Kes

Prof. Dr. rer. Nat. Rosari Saleh

Penulis:

Devie Rahmawati; Giri Lumakto; Rizki Ameliah; Mila Viendyasari; Rangga Adi Negara; Aisyah Adinda; Syavia Bachna

Editor: Rienzy Kholifatur

Desain: Sandra

PENERBIT:

Program Studi Hubungan Masyarakat

Program Vokasi Universitas Indonesia

DAFTAR ISI

KATA PENGANTAR

Segala Puji dan Syukur kami panjatkan selalu kepada Tuhan Yang Maha Esa atas Rahmat, Taufiq, dan Hidayah yang sudah diberikan sehingga kami bisa menyelesaikan modul panduan yang berjudul "*Cyber Crime*" dengan tepat waktu. Tujuan dari penulisan modul ini tidak lain adalah untuk membantu para masyarakat di dalam memahami seperti apa *Cyber Crime* yang ada di dunia digital, sehingga harapannya masyarakat bisa mengetahui tahapan apa saja yang harus di lakukan.

Modul ini juga akan memberikan informasi secara lengkap mengenai pengertian, macam, tujuan, dan banyak contoh dari *Cyber Crime.*

Kami juga sadar bahwa modul yang kami buat masih tidak belum bisa dikatakan sempurna. Maka dari itu, kami meminta dukungan dan masukan dari para pembaca, agar kedepannya kami bisa lebih baik lagi di dalam menulis sebuah modul.

Jakarta, 20 November 2022

Tim Penulis

Cyber Crime

1. Pengertian & sejarah cyber crime

Data, media, atau komunikasi inovasi telah meningkatkan kesejahteraan domestik dan global. Kemajuan teknologi komunikasi dan informasi yang cepat ini menyebabkan perubahan besar dalam keadaan sosial, keuangan, atau budaya. Karena teknologi internet terus berkembang, memang mungkin potensi kejahatan dunia maya atau beberapa bentuk lain seperti teror Web dapat tumbuh. Ada beberapa kasus yang melibatkan kejahatan dunia maya di Indonesia, termasuk pencurian identitas, peretasan situs, pencurian banyak informasi pribadi lainnya, terutama email, dan manipulasi data menggunakan kredensial semu.

Menurut Andi Hamzah, kejahatan siber memang merupakan jenis kejahatan yang didefinisikan sebagai penggunaan komputer yang melanggar hukum dalam artikelnya "Aspek-aspek pidana di bidang komputer" (1989). Salah satu penjelasan untuk kejahatan dunia maya adalah sebagai berikut:

1. Menurut Girasa pada tahun 2002 mendefinisikan kejahatan siber sebagai tindakan yang menggunakan teknologi komputer sebagai komponen utama.

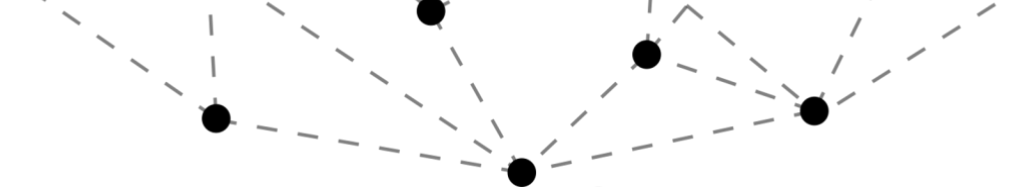
2. Menurut Tavani tahun 2000 memberikan definisi cybercrime sebagai berikut: situasi dimana aktivitas kriminal terbatas pada penggunaan cyber technology dan terjadi di dunia maya.

Tidak mungkin menerapkan Cyber Law atau Cyber Hukum untuk memerangi Cyber Crime. Cyberlaw adalah bidang hukum yang, dalam bentuknya yang paling dasar, menjunjung tinggi prinsip konstitusional apa pun yang memiliki hubungan dengan orang atau entitas lain, atau bahkan sistem pemerintahan lain. Ini juga memungkinkan orang untuk mengakses teknologi ketika mereka online dan terlibat dalam aktivitas "cyber" atau "maya". Hukum Dunia Maya kemungkinan besar sekarang merupakan cabang dari cyberlaw, seperti yang mungkin Anda yakini saat ini.

Istilah hukum cyber digambarkan sebagai "padanan kata" dalam Cyberlaw, yang saat ini digunakan oleh setiap negara di dunia dalam sistem peer review terkait potensi keuntungan finansial dari penggunaan TI. Hukum Mayantara, Hukum Dunia Maya, dan Hukum TI adalah sistem peradilan tingkat atas lainnya yang digunakan (UU Sistem Informasi). Menurut standar pendidikan, kata-kata mutiara terkait siberan hukum terus digunakan. Tidak akan hanya ada satu sistem hukum yang mapan di Indonesia, tepatnya. Di mana metode ini digunakan? Sistem Teknologi Informasi, Informasi, dan Telematika (Telekomunikasi dan Informatika).

Seperti menurut pemikiran umum, cyberlaw bervariasi dari luas dan batasan dalam hukum ". Meskipun menjadi terutama virtual, siber dapat dianggap hanya sebagai antara dan perbuatan untuk undang-undang. Meskipun peralatan yang digunakan untuk mengeksekusinya benar-benar sebagian besar adalah digital, perang dunia maya memang merupakan konflik virtual yang juga diperebutkan dengan panas. Dalam gugatan ini, termohon dari suatu perkara tertentu harus dinyatakan sebagai orang perseorangan yang telah lulus ujian hukum formal.

Serangan pertama di dunia diduga dilakukan pada tahun 1834 ketika segelintir perampok menggunakan Sistem Telegraf Prancis dan



memperoleh data dari pasar saham. Setelah itu ketika, selama tahun 1878, bisnis Bell, Seluler Awal-Perusahaan Telepon, memindahkan sekelompok bayi anak-anak dari telegraf listrik New York hanya untuk ke-4 berturutturut, dan 2 tahun setelah Bell menemukan mesinnya, secara efektif mengarahkan dan memutuskan panggilan pelanggannya. Terakhir tetapi tidak bertahan lama, selama tahun 1955, David Condon dari Peretas Telepon orientasi teoritis mengenai layanan jaringan telepon menggunakan program tv "Davy Crockett Cat" dan "Canary Bird Call Flute." Node menerima sinyal rahasia, berpikir bahwa klien memang seorang pelajar, dan menghubungkannya ke operator jauh.

Serangan pertama di dunia diduga dilakukan pada tahun 1834 ketika segelintir perampok menggunakan Sistem Telegraf Prancis dan memperoleh data dari pasar saham. Setelah itu ketika, selama tahun 1878, bisnis Bell, Seluler Awal-Perusahaan Telepon, memindahkan sekelompok anak kecil dari telegraf listrik New York hanya untuk ke-4 berturut-turut, dan 2 tahun setelah Bell menemukan mesinnya, secara efektif mengarahkan dan memutuskan panggilan pelanggannya. Last but not least, pada tahun 1955, David Condon dari Peretas Telepon mengeksplorasi teori tentang bagaimana fungsi jaringan telepon dengan menggunakan program televisi "Davy Crockett Cat" dan "Canary Bird Call Flute." Komputer menerima pesan rahasia, dengan asumsi pengguna adalah pelajar, dan menghubungkan mereka ke operator jauh.

Dinas Rahasia AS-Undang-Undang Pencegahan Kejahatan Komprehensif Amerika Serikat memberikan kesempatan kepada masyarakat dan bisnis bagi Dinas Rahasia untuk mengeksplorasi ecommerce pada tahun 1984. 1988 - The Morris Worm - Robert Morris membahas apa yang akan dianggap sebagai cacing pertama hanya di Internet. Cacing diambil dari sistem MIT seperti itu untuk menunjukkan bahwa pencipta adalah shah asli. Program Kuda Troya, 1989 Sebuah file

yang tampaknya merupakan paket info AIDS dikirim ke majalah online berbahasa Inggris dari ribuan Aids dan teman-teman lainnya.

1994 – Manajer Datastream Cowboy and Kuji di Rome Air Production Centre, fasilitas pengujian Angkatan Udara AS telah memasang kata sandi “sniffer” di jaringannya, yang membahayakan lebih dari 100 profil pengguna. Penyelidik menemukan bahwa ada dua peretas di balik serangan itu, yang diidentifikasi sebagai Datastream Cowboy dan Kuji. 1995 - Vladimir Levin—Pengembang perangkat lunak Rusia Vladimir Levin meretas dari apartemennya di Saint Petersburg ke mesin

IT Citibank New York dan mengizinkan sejumlah transfer ilegal, yang pada akhirnya menghubungkan rekening di seluruh dunia dengan perkiraan sekitar $10 juta. 1999 - Virus Melissa Virus-A menginfeksi catatan Microsoft Word, mengirimkan dirinya sendiri melalui email sebagai lampiran secara otomatis. Ini mengirimkan ke 50 nama pertama yang disebutkan dalam kotak alamat email Outlook dari perangkat yang terinfeksi. 2000 - Barry Schlossberg, alias Lou Cipher, berhasil memeras $ 1,4 juta dari CD Universe untuk layanan yang diberikan kepada peretas Rusia dalam upaya untuk menangkapnya.

Dinas Rahasia AS-Undang-Undang Pencegahan Kejahatan Komprehensif Amerika Serikat memberikan kesempatan kepada masyarakat dan bisnis bagi Dinas Rahasia untuk mengeksplorasi ecommerce pada tahun 1984. 1988 - The Morris Worm - Robert Morris membahas apa yang akan dianggap sebagai cacing pertama hanya di Internet. Cacing diambil dari sistem MIT seperti itu untuk menunjukkan bahwa pencipta adalah shah asli. Program Kuda Troya, 1989 Sebuah file yang tampaknya merupakan paket info AIDS dikirim ke majalah online berbahasa Inggris dari ribuan Aids dan teman-teman lainnya.

2002 telah melihat operasi debut Online Attack-A DDoS, yang dengan satu jam menyerang hampir seluruh Internet dengan menjatuhkan 13 Domain Name System root system (DNS). Penggunaannya yang biasa benar-benar tidak berubah. ChoicePoint-A

warga di Nigeria telah menggunakan sistem ini selama lebih dari 41 tahun, namun bisnis ini sendiri telah mengajarkan 35.000 warg mengenai prinsip-prinsip dasarnya. 2006 telah melihat penyitaan lebih dari 45 juta informasi kartu debit dan kredit di TJX, sebuah perusahaan ritel berbasis ritel Massachusetts, oleh sekelompok kelompok main hakim sendiri Mesoamerika. Ini menggunakan salah satu kartu kredit dan debit terbesar untuk melakukan pembelian dari Wal-Mart. 2008 telah melihat entri spyware ke jaringan komputer Heartland dengan menggunakan Cross - site scripting.

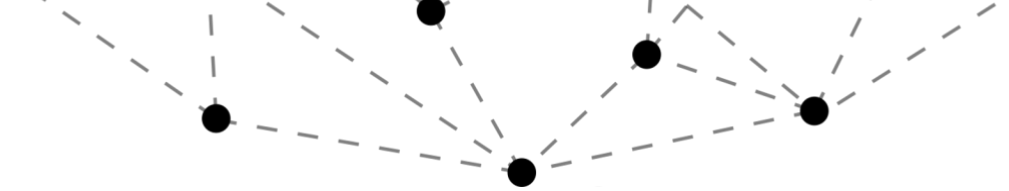
Stuxnet Worm-Bom, bahaya lunak pertama di seluruh dunia tahun 2010, adalah bahaya perangkat lunak yang benar-benar dapat mengganggu mekanisme kontrol yang digunakan untuk mengawasi pabrik produksi. 2011 - Serangan siber Epsilon-A di Epsilon memberi pelanggan kemampuan akses email yang melarang penggunaan satu miliar akun email pribadi, seperti Best Buy dan JPMorgan Chase. 2013-2015 - Peretasan Bank Global - Dan lebih dari 100 organisasi di seluruh dunia memiliki akses ke informasi yang berasal dari komunitas peretas tergantung dalam bahasa Rusia. 2015 - Pada smartphone Android, Lock Pin mengirimkan nomor pin dan menginginkan $500 dari klien untuk menggunakan layanan, menuduh bahwa informasi pribadi memang telah dicuri hingga 78,8 juta pengguna aktif baik saat ini maupun sebelumnya. WikiLeaks mengakuisisi dan membebaskan partai Dem dari Komite Nasional Demokrat selama 2016 jauh sebelum pemilihan presiden AS.

Rupanya, belum terjadi pelanggaran HAM maya yang signifikan hingga tahun 1980. Satu pengguna memegang laptop orang lain untuk melihat, memasukkan, atau menangani informasi dan data pribadi. Individu pertama yang juga diakui berjuang untuk teror Maya adalah Ian Murphy, lebih dikenal sebagai Kapten Zap, dan itu terjadi pada tahun 1981. Itu memang memiliki kesepakatan dengan perusahaan kereta api

Amerika yang mengontrol waktu lokal internalnya sehingga pelanggan masih dapat melakukan panggilan tak terbatas di mana saja saat ini. Seperti biasa, peretas selesai dengan cara yang berubah dari minggu ke minggu. Meskipun fokus utama dari operasi telemarketer perusahaan memang bank, situs, atau mungkin warga negara swasta tanpa implementasi yang cepat juga. Saat ini, perbankan online sangat luas tetapi menimbulkan risiko yang besar. Misalnya, peretas dapat memasukkan kata sandi dan identitas untuk dimasukkan, atau mereka dapat memperoleh frasa entri dari akun kartu kredit. Konsekuensi ini adalah tidak ada yang bisa bertukar identitas atau melakukan pembayaran online dengan ponsel orang lain!

Frasa "kejahatan dunia maya" ini pertama kali digunakan pada tahun 1988 sebagai referensi "serangan dunia maya." Dengan berpartisipasi dalam kejahatan dunia maya, populasi yang lebih luas memang memiliki kapasitas untuk membuat virus dan worm yang membahayakan perangkat lunak komputer dan oleh karena itu dapat menutup sekiranya 10% untuk mesin terbesar di seluruh penjuru dunia yang telah terhubung ke jaringan internet. Kejahatan jenis ini terus meningkat di dunia maya dengan adanya kemajuan teknologi saat ini serta semakin banyak kebutuhan manusia. Namun demikian, telah ditunjukkan bahwa kejahatan dunia maya khusus ini memiliki deskripsi yang sangat sederhana dan efektif. Skenario itu melalui banyak agen federal untuk mengambil penyidikan.

Pada era ini, setiap penduduk yang lebih luas lebih nyaman karena penggunaan internet mereka, dan terutama media sosial telah berkembang menjadi prasyarat. Kita harus terus berhati-hati saat menggunakan web dan media sosial karena saat ini, semua orang yang menggunakan web berisiko menjadi korban atas kejahatan media sosial. Apa sebenarnya kejahatan dunia maya itu? Kejahatan media sosial



mengacu pada salah satu dari banyak jenis yang melibatkan akses yang tidak tepat ke transfer informasi. Dalam istilah lain itu, "teror asia tengah" mengacu pada tindakan apa pun yang sebelumnya telah merugikan jaringan komputer, atau "tindakan teroris di dalam ranah Digital." Sebagaimana mestinya, pesan asia tengah mencakup peringatan terhadap mesin yang saat ini terhubung ke Web.

Meskipun sebagian besar peretas ada di sini untuk mengambil uang tunai dari orang lain, sebenarnya ada perbedaan yang jelas antara berbagai jenis peretas. Memang penting untuk mendapatkan gambar yang lebih tajam: peretas yang ingin menghasilkan transmisi. Itu terjadi, misalnya setiap kali bank dibuat, hanya untuk mendeteksi kesalahan dan kebocoran di dalam platform manajemen bank. Peretas yang benar-benar nyata yang berinteraksi dengan sistem untuk menghasilkan hasil yang menjanjikan.

Kejahatan siber tidak hanya dilakukan kepada keisengan semata saja; sebaliknya, itu dilakukan dengan berbagai tujuan dalam pikiran. Pada awalnya, tujuan kejahatan dunia maya adalah untuk mengidentifikasi peretasan atau bahkan pelanggaran lainnya, tetapi kemudian seiring berjalannya waktu, menjadi jelas bahwa kejahatan memiliki motif yang jauh lebih parah, seperti kemungkinan menyebabkan kerugian psikologis dan finansial bagi para korban. Salah satu kasus pelecehan seksual berat yang paling sering terjadi di Indonesia ketika terjadi kontroversi jejaring sosial. Rekayasa sosial/social engineering adalah metode untuk menangani orang-orang yang memanfaatkan kelemahan seseorang untuk mendapatkan akses ke data sensitif dan penting secara efektif.

Banyak orang termasuk nasabah bank menjadi korban kejahatan dunia maya. Di masa pandemi, semua aktivitas dilakukan secara online sehingga nasabah perbankan dapat memanfaatkan peluang perbankan

digital secara maksimal. Pelanggan harus berhati-hati agar tidak menjadi mangsa kejahatan dunia maya dan meningkatkan keamanan data. Sebenarnya, ada banyak cara penjahat dunia maya dapat meretas data pribadi. Pertama, penjahat digital sangat berhati-hati terhadap pelanggan/target yang ingin mereka serang. Penjahat dunia maya memilih target dan secara terbuka menghubungi customer service (CS) bank melalui media sosial pribadi target. Dengan cara ini, penjahat dunia maya dapat memperoleh data mentah dari individu, seperti nomor ponsel, nama, dan tempat lahir, yang tidak sulit ditemukan di Internet. Menurut penulis tidak sulit menemukan hal seperti itu di Internet. Terakhir, penjahat dunia maya menyamar atau berpura-pura menjadi pegawai bank dengan menjangkau pelanggan sasaran mereka melalui percakapan media sosial, pesan teks, dan bahkan panggilan telepon.

Dari segi hukum, e-law belum memenuhi standar dan persyaratan hukum konvensional. Meskipun fiktif, aktivitas komputer dapat diklasifikasikan sebagai proses komersial dan hukum yang jelas. Aktivitas komputer adalah aktivitas hipotetis yang memiliki implikasi yang sangat negatif, bahkan jika itu sepenuhnya elektronik. Karena itu, pelamar juga harus memiliki kualifikasi untuk bekerja dalam kapasitas hukum.

Ciri-ciri Kejahatan Sosial Media adalah sebagai berikut:

1. Kejahatan Bertingkat

Sulit untuk mengidentifikasi pelaku dan hukum yang berlaku karena terorisme dunia begitu luas dan transnasional.

2. Jahat

Tidak jelas bagaimana hukum pidana Maya berhubungan dengan kebutuhan yang didefinisikan dengan jelas.

3. Pelanggaran

Ada dan akan selalu ada kejahatan di dunia ini. Beberapa dari mereka adalah wanita dan anak-anak, kebanyakan.

4. Pendakian Bermodus

Modus operandi kejahatan dunia maya. Hanya mereka yang memiliki komputer, seperangkat alat pemrograman, dan beberapa pengetahuan tentang dunia Maya yang dapat memahami di mana mode lazim.

5. Istilah kerusakan

Ini mungkin berfungsi penuh atau tidak. Misalnya, waktu, uang, mata uang, barang, harga eceran, dan mungkin informasi yang tidak lengkap.

Beberapa langkah penting yang perlu diambil oleh setiap negara untuk memerangi jenayah siber ialah:

1. Pemodenan undang-undang jenayah dan prosedur negara selaras dengan konvensyen undang-undang jenayah antarabangsa

2. Penambahbaikan sistem keselamatan rangkaian komputer negara mengikut piawaian antarabangsa

3. Meningkatkan kesedaran dan kepakaran pegawai penguatkuasa undangundang dalam mencegah, menyiasat dan menilai kes berkaitan jenayah siber

4. Meningkatkan kesedaran orang ramai tentang jenayah siber dan kepentingan mencegahnya

5. Memperkukuh kerjasama dua hala, serantau dan pelbagai hala antara negara, termasuk melalui perjanjian ekstradisi dan perjanjian bantuan bersama, dalam memerangi jenayah siber

2. Contoh kejahatan siber

Teknologi berkembang pesat tetapi ia tidak mengecualikan kita daripada semua jenis kejahatan siber di alam siber. Secara umumnya, tujuan siber kejahatan ini adalah untuk mendapatkan maklumat dan memanipulasi data secara sah, yang dilakukan melalui pelbagai tindakan yang wujud dalam kejahatan siber. Berikut adalah contoh kejahatan siber:

- Masuk ke ruang komputer dan gunakan jaringan secara legal.

  Jenis terorisme ini dilakukan dengan menyusup ke jaringan komputer tanpa persetujuan pemiliknya. Secara umum, tujuan dari pembunuh virtual dalam hal ini adalah untuk melindungi atau mengumpulkan informasi sensitif, berbeda dengan mereka yang melakukan tindakan terorisme di dunia nyata semata-mata untuk tujuan menyembunyikan kemampuan mereka dalam data meretas dan mendapatkan akses ke jaringan tanpa sepengetahuan pemiliknya.

- pemalsuan data

  Jenis kejahatan dunia maya ini biasanya digunakan untuk memalsukan data yang dianggap penting oleh sebagian orang, meskipun data tersebut disimpan sebagai dokumen tidak tertulis di Internet. Biasanya, kejahatan dunia maya ini dilakukan untuk tujuan penjualan data melalui e-commerce.

- Konten ilegal

  Cybercrime biasanya hanya dilakukan untuk membuat konten yang populer dan dibicarakan di masyarakat. Penjahat dunia maya mencuri data untuk dijadikan sebagai sumber informasi palsu, tidak etis, dan bahkan ilegal di Internet. Sebagai contoh, saat ini banyak postingan palsu yang hanya bertujuan untuk melecehkan

media sosial dan menjadi populer di kalangan manusia yang tidak memiliki rasa tanggung jawab.

- Spionase sosial media

  Jenis kejahatan ini berbeda dari yang lain dalam spionase dunia maya dapat digunakan selamanya dan dapat mematikan jika disalahgunakan, karena jenis kejahatan ini dirancang untuk memata-matai berbagai pihak dengan meretas sistem komputer ilegal.

- Retakan

  Jenis kejahatan ini ditujukan untuk menghancurkan sistem keamanan komputer. Biasanya, seorang penjahat melakukan kejahatan jika ia berhasil mendapatkan akses ke sistem komputer.

Saat melakukan suatu tindakan, peretas menggunakan langkah-langkah berikut (Gregory, 2005):

sebuah.

- Melacak

  Informasi target diperlukan pada saat ini. Pemindaian ini adalah upaya untuk menemukan lubang untuk menonaktifkan sistem.

- Menghitung

  Pelajari sistem secara menyeluruh, cari akun pengguna aktif, jargon siang hari yang valid, dan aplikasi sistem aktif.

- Mengakses

  Dapatkan lebih banyak data untuk mencoba dan mengakses target. Ini termasuk pengintaian dan pengambilan kata sandi, tebakan kata sandi, dan buffer overflows.

- Hak Istimewa yang Diperpanjang

  Jika Anda baru saja mendapatkan kata sandi pengguna pada langkah sebelumnya, langkah ini akan mencoba untuk mendapatkan hak administrator jaringan dengan meretas atau menggunakan kata sandi.

- Pencurian

  Proses pengumpulan informasi terus mengembangkan mekanisme yang diperlukan untuk mendapatkan akses ke sistem yang dapat dipercaya. Termasuk adanya informasi terkait kepercayaan dan penulisan teks biasa dalam registri, file konfigurasi, dan data pengguna.

- Lagu terakhir
- Setelah sistem menyelesaikan sedikit kontrol terakhirnya, jadikan jalur sebagai prioritas utama Anda. Ini termasuk merobek-robek log jaringan dan menggunakan alat yang rentan seperti berbagai rootkit dan torrent file.

- Lakukan pintu belakang

  Backdoors dibuat di berbagai bagian sistem untuk memfasilitasi login dengan membuat akun pengguna palsu, menjadwalkan pekerjaan batch, memodifikasi file startup, termasuk layanan remote control dan sistem pemantauan.

Setiap tindakan kriminal pastinya akan dikenakan hukum, termasuk kejahatan *cyber crime*. Untuk mengatasi kejahatan virtual, ternyata negara telah membuat *cyber law*/hukum siber untuk para pelaku kejahatan virtual. Cyber law memiliki aspek hukum yang telah mencakup banyak hal, maupun secara individu atau subjek hukum yang digunakan untuk memanfaatkan teknologi internet.

Cyber law ini memiliki fungsi, sebagai berikut : menguranginya kejahatan virtual, melindungi data pribadi, serta menjamin kepastian hukum.

3. Jenis-jenis cyber crime

- **Kejahatan *phising***

  Kegiatan yang memiliki tujuan untuk mendapatkan suatu data dan informasi rahasia pengguna, hal tersebut dilakukan dengan cara menggunakan situs web palsu yang menyerupai dengan tampilan asli dari web pengguna sebelumnya. Adapun tips untuk meminimalisir kejahatan *Phising,* yaitu :

  - ➔ Jangan mengirim informasi/data sensitif melalui e-mail, karena biasanya perusahaan tidak akan meminta data/informasi sensitif dengan cara melalui e-mail atau sarana yang lain.
  - ➔ Gunakan anti virus yang baru, jangan pernah klik apapun saat ada pesan (e-mail) yang memiliki ciri-ciri phishing.
  - ➔ Segera melakukan konfirmasi terhadap pihak yang terkait, jika sudah memiliki permintaan yang diluar kendali/mencurigakan.
  - ➔ Jangan memasukan *password* dan *user ID* pada situs/halaman web yang bisa terbuka secara otomatis.
  - ➔ Hati-hati dalam mengunduh *attachment email*, hal tersebut dapat dipastikan bisa menyebabkan virus yang meretas data sensitif.

- **Kejahatan *carding***

Suatu kejahatan yang bertujuan untuk mencuri nomor kartu kredit, hal tersebut dilakukan dengan cara situs legal/spammer, lalu pelaku dimanfaatkannya untuk pembelian gift card prabayar. Tidak sampai disitu, kartu gift tersebut dijual dengan tujuan agar mendapatkan sejumlah uang. Adapun tips untuk meminimalisir kejahatan *Carding*, yaitu :

- ➔ Pastikan untuk menjaga selalu menjaga kartu agar tetap aman, maupun saat transaksi *online* atau *offline.*
- ➔ Selalu perhatikan petugas yang menggesek kartu tersebut, apakah menggunakan mesin EDC atau tidak. Pastikan kartu tersebut hanya digesek satu kali saja dan tidak boleh lebih dari satu kali, apalagi pada mesin yang berbeda dengan mesin yang sebelumnya.
- ➔ Pilihlah situs belanja online yang dipercaya, bahkan yang memberikan sebuah sistem keamanan ganda untuk pengguna kartu kredit. Contohnya dengan memfasilitasi nomor OTP bagi pengguna kartu kredit, agar proses transaksi jauh lebih aman.
- ➔ Rahasiakan *Card Verification Value* dan nomor kartu kredit tersebut. Jangan coba-coba untuk memberitahu kedua hal tersebut kepada keluarga, apalagi orang lain.
- ➔ Jangan melakukan transaksi menggunakan internet publik, apalagi saat mengakses situs perbelanjaan *online.* Hal tersebut sudah dipastikan bahwa wifi publik belum terjamin sistem keamanannya.

➔ Pastikan merobek terlebih dahulu surat tagihan kartu kredit sebelum membuangnya, dengan begitu tidak ada yang bisa melihat data pribadi.

- **Kejahatan *pharming***

  Tindakan perintah yang langsung mengarahkan pengguna/korban untuk ke situs web palsu. biasanya, pelaku memasang malware di situs palsu tersebut. Dengan begitu, pelaku akan lebih mudah mengakses perangkat korban dengan ilegal. Adapun tips untuk meminimalisir kejahatan *pharming*, yaitu :

  ➔ Aktifkan 2FA, merupakan suatu metode keamanan yang memiliki dua langkah verifikasi baik di website, platform, atau aplikasi.

  ➔ Berhati-hati untuk mengklik link yang beredar pada internet, pastikan link tersebut sudah memiliki sertifikat SSL. Bagaimana kita tahu jika link tersebut sudah bersertifikat SSL? pastinya ada perbedaan, yaitu kamu bisa melihat terlebih dahulu link tersebut, jika diawali HTTPS, link tersebut sudah bisa dipastikan memiliki sertifikat SSL.

  ➔ Gunakan server DNS yang terpercaya, gunakan DNS layanan khusus/privat dengan begitu akan jauh lebih aman. DNS sendiri telah menyediakan ISP *(Internet Service Provider).*

  ➔ Pastikan untuk mengunduh file pada website yang sudah memiliki jaminan keamanan, karena pharming sering terjadi dari file yang diunduh pada internet.

- **Kejahatan *sniffing***

  Suatu tindakan menyadap yang memiliki tujuan untuk mengumpulkan berbagai data/informasi dalam perangkat korban. Tidak hanya itu saja, pelaku juga akan mengakses berbagai aplikasi

yang memiliki data penting. Adapun tips untuk meminimalisir kejahatan *sniffing*, yaitu :

➔ Menggunakan keamanan enkripsi WPA2-PSK pada hotspot/wifi. hal tersebut bisa meningkatkan sistem keamanan, karena dengan begitu hanya individu yang ditentukan yang mampu terhubung ke jaringan tersebut.

➔ Perbaruilah browser pada versi terbarunya., karena bisa dipastikan keamanan browser lama sudah tidak terjamin keamananya.

➔ Berhati-hati untuk mengklik link yang beredar pada internet, pastikan link tersebut sudah memiliki sertifikat SSL.

Bagaimana kita tahu jika link tersebut sudah bersertifikat SSL? pastinya ada perbedaan, yaitu kamu bisa melihat terlebih dahulu link tersebut, jika diawali HTTPS, link tersebut sudah bisa dipastikan memiliki sertifikat SSL.

- **Kejahatan *social engineering***

Serangan social engineering telah menimbulkan ancaman keamanan yang serius bagi dunia maya. Namun, di sana banyak yang belum kita ketahui mengenai apa dan bagaimana mengarah pada keberhasilan serangan rekayasa sosial. Makalah ini mengusulkan model konseptual yang memberikan perspektif integratif dan struktural untuk menggambarkan cara kerja serangan rekayasa sosial. Tiga entitas inti (mekanisme efek, kerentanan manusia, dan serangan metode) diidentifikasi untuk membantu pemahaman tentang bagaimana serangan rekayasa sosial berlaku. Kemudian, di luar Ruang lingkup yang akrab, kami

menganalisis dan membahas mekanisme efek yang melibatkan 6 aspek (persuasi, sosial pengaruh, kognisi & sikap & perilaku, kepercayaan dan penipuan, bahasa & pikiran & keputusan, emosi dan pengambilan keputusan) dan kerentanan manusia yang melibatkan 6 aspek (kognisi dan pengetahuan, perilaku dan kebiasaan, emosi dan perasaan, sifat manusia, ciri-ciri kepribadian, karakter individu), masing-masing.

Rekayasa sosial telah menjadi taktik yang sangat umum di komunitas peretas sejak 1970-an. Fokus pada jejaring sosial daripada pidato terkomputerisasi tradisional seperti penggunaan kekerasan dan eksploitasi perangkat lunak

Pemimpin redaksi Xiali Hei mengawasi organisasi proyek naskah saat ini dan memastikan bahwa itu siap untuk diterbitkan. Menggunakan sifat manusia tanpa perlu dilindungi oleh firewall atau program antivirus dengan pasangan kunci Mendalam untuk menyerang atau diserang melalui Hambatan Keamanan. Akibatnya, tidak ada sistem komputer yang tidak mendukung manusia atau memperhitungkan faktor manusia dalam tubuh; Sebaliknya, faktorfaktor ini jelas rentan atau cukup besar untuk diubah menjadi kerentanan keamanan oleh On-the-spot Penyerang. Hal ini tidak benar, karena faktor manusia yang mencari rente menyebabkan rekayasa sosial menjadi Siberia Universal Siberian Keamanan. Dalam beberapa keadaan, anggota Merekayasa serangan sosial mungkin mengangkat telepon dan berpura-pura sebagai orang luar untuk mendapatkan informasi waktu nyata. Rekayasa sosial Ancaman menjadi lebih serius sebagai akibat dari kemajuan teknologi baru dan perkembangan dunia maya. Situs untuk Jejaring Sosial (SNSs), komunikasi seluler,

Industri Internet, dan Internet of Things (IoT) tidak hanya menghasilkan sejumlah besar informasi yang sangat sensitif tentang manusia dan hewan, tetapi juga sejumlah besar saluran dan permukaan serangan. Lingkungan kantor yang tidak mengalami perdebatan (seperti perangkat bawah itu sendiri, kantor jarak jauh, dll.) diuji hingga mengisolasi daerah tersebut dari berbagai kondisi cuaca dan menghasilkan lebih banyak peluang serangan. Pengumpulan informasi terhambat oleh penyebaran informasi yang mudah. Untuk memperoleh lebih banyak serangan rekayasa sosial yang dapat dicreditkan dan ditargetkan, target spesifik dapat dipilih dengan cermat. Kelompok korban besar dapat terhubung pada hari yang sama, dan beberapa pompa bah yang tidak stabil dapat digunakan untuk memicu Serangan semi-otomatis. Teknologi seperti pembelajaran mesin dan kecerdasan buatan dapat membuat konflik sosial lebih agresif dan efektif. Rekayasa jejaring sosial bertarget yang berskala besar, otomatis, dan kabur dimungkinkan. Kepastian kemajuan sosial sekarang menjadi konsep yang gigih, ada di mana-mana, dan serius.

Pekerjaan sangat penting untuk memahami bagaimana melaksanakan tugas dan terus beroperasi untuk melindungi diri dari dampak sosial. Inilah yang menyulitkan kontributor untuk berkontribusi, sebagai berikut:

- Model integratif dan struktural untuk menggambarkan bagaimana rekayasa sosial bekerja dan terus berfungsi.
- Ada kewenangan yang cukup untuk memperoleh informasi tentang keadaan darurat rekayasa sosial.
- 30+ mekanisme efek yang mempengaruhi enam kategori.
- 40+ manusia yang mewakili enam spesies berbeda.

- Studi 16 skenario untuk evaluasi ulang sosial (termasuk 13 metode serangan tipe)

One-Time Password adalah salah satu contoh teknik untuk memanipulasi aspek psikologis perilaku manusia agar berhasil memperoleh data atau informasi penting (OTP). Interaksi dapat terjadi di berbagai saluran komunikasi, termasuk telepon, sms, email, pesan langsung, platform Whatsapp, atau bahkan dapat berlangsung tatap muka dengan target atau musuh. Ada beberapa saran untuk mengurangi penggunaan manipulasi psikologis, khususnya:

➔ Petugas bank harus meninjau isi gedung, mirip dengan bagaimana pengunjung harus memeriksa kartu identitas mereka lebih teliti sebelum memasuki gedung.

➔ Bank harus menyediakan lokasi untuk penandatanganan dan penandatanganan dokumen yang aman secara terus menerus.

➔ Dokumen lain juga harus dihancurkan untuk mencegah pengambilan oleh individu yang terlibat dalam penyelaman sampah.

➔ Perangkat yang sudah terkoneksi dengan internet harus mengambil tindakan protektif dengan menggunakan tulisan ala sandi.

● **Penipuan online**

Tindakan yang dilakukan secara online antara lain mencakup ecommerce yang memanfaatkan penyedia layanan internet tertentu. Fakta bahwa ini dilakukan adalah karena ia memiliki

berbagai tujuan, termasuk menghapus pengguna, mendapatkan hadiah pengguna, dan melindungi informasi pengenal pribadi yang telah bocor. Ada beberapa saran untuk mengurangi perundungan internet, khususnya:

- ➔ Pelajari cara mengenali phishing, bentuk penipuan online lainnya, dan tanda-tanda peringatan penipuan.
- ➔ Perbarui sistem operasi, browser web, dan aplikasi komputer Anda ke versi terbaru.
- ➔ Pelajari dasar-dasar manajemen siberia.
- ➔ Jangan gunakan kata sandi yang sama untuk banyak akun. Kobalt untuk membuat sandi kata yg tidak dapat ditulis ulang serta hindari dengan menggunakan nama, tanggal, atau kata umum. Belum pernah saya bertukar kata-kata amplas dengan seseorang pada khususnya.
- ➔ Jangan memberikan informasi pribadi di situs web yang tidak ditranskripsikan. Hanya perhatikan situs web yang dimulai dengan "https" ("s" berarti mereka aman). Mereka mengubah informasi menjadi kode yang mendeteksi penjahat potensial.

- **Peretas Situs**

  Ada kemungkinan seseorang akan mengklaim kepemilikan sebuah website setelah menerima informasi atau data yang dapat diamankan. Orang itu kemudian dapat menjual situs web kepada orang lain dengan tujuan menghasilkan uang dalam jumlah besar. Ada beberapa saran untuk mengurangi terorisme di seluruh situs, khususnya:

- ➔ Pantau teknik kejahatan dunia maya terbaru sehingga dapat membantu masyarakat memahaminya saat mereka meletakkan hukum.
- ➔ Menghasilkan perangkat lunak anti-virus dan memperbarui perangkat lunak, dapatkan oleh pembaruan umumnya yang meningkatkan keamanan dan menghapus bug.
- ➔ Untuk tujuan meningkatkan kemampuan perangkat lunak, perangkat keras juga harus terus diperbarui.
- ➔ Jangan pernah membuka email atau pesan yang berisi katakata tidak senonoh.
- ➔ Menghambat jaringan publik dan menonaktifkan Bluetooth saat tidak digunakan.
- ➔ Kata sandi harus dibuka kembali dengan tenang.

- **OTP Fraud (begal rekening)**

  Tindakan yang dilakukan secara pribadi atau oleh orang yang bertindak jujur memerlukan menjadi pemegang rekening bank dan meminta kode keamanan, PIN, MPIN, dan OTP. Untuk mendapatkan informasi dari korban dan untuk mendapatkan keuntungan finansial yang terpisah, penyalur menghubungi korban melalui berbagai media sosial. Ada beberapa saran untuk mengurangi Penipuan OTP, khususnya:

  - ➔ Jangan pernah memberitahukan nomor PIN atau OTP anda kepada siapapun.
  - ➔ Lembaga lain seperti bank tidak memerlukan kredensial seperti OTP, PIN, nomor CVV, atau kredensial lainnya.

- ➔ Jika korespondensi semacam ini diberikan kepada seseorang, orang itu akan diberikan uang dari rekening mereka.
- ➔ Jika orang lain meminta OTP, PIN, nomor CVV, atau jenis kode rahasia lainnya, jangan memindahkan atau merusak panggilan.
- ➔ Jangan langsung percaya penelepon tanpa polling jika telah menginstal Truecaller dan muncul nama sebagai manajer bank atau nama bank.

- **Cybercrime: Jenis dan Penggolongan**

Mulailah dengan mencatat berbagai contoh kejahatan dunia maya melalui dunia maya (internet) untuk mendorong orang memahami apa sebenarnya kejahatan dunia maya itu dan bagaimana cara memeranginya. Kejahatan dunia maya adalah kategori yang sangat luas yang semakin tidak stabil dari waktu ke waktu.

Kekerasan terkait internet telah menjadi masalah serius saat ini, antara lain;

a. **Eksploitasi Dunia Sosial Media *(Cybercrime)* ;**

Cukup memakai computer dan menghubungkan ke jaringannya, atau menggunakan komputer yang diperlukan agar kejahatan ini terjadi. Hal ini juga bisa terjadi di dunia maya dengan sasaran serupa lainnya.

1. Cyberpiracy adalah penerapan metode ilmiah dalam komputer untuk secara diam-diam mencegat komunikasi, mencuri

informasi, atau menyebarkan informasi itu atau program itu melalui penjaringan computer. Konteks: Menggunakan teknologi peer-topeer untuk mendistribusikan file MP3 secara online.

2. Cybertrespass adalah praktik menggunakan teknologi komputer untuk mendapatkan peningkatan akses ke sistem komputer orang lain atau organisasi; Ini terjadi di situs web yang menggunakan sandboxing. Contoh Kasus: Meluncurkan DoS (Denial of Service) di situs web.

3. Cybervandalism adalah penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi informasi elektronik atau untuk mencuri data komputer.

Contoh Kontekstual: melakukan serangan DoS (Denial of Service) pada situs web dan membuat virus SASSER

b. **Perbedaan antara kejahatan dunia maya dan kejahatan kekerasan yang terhubung dengan dunia maya (cyber related crime);**

Berlimpah tindakan kekerasan yg melibatkan komputer teknologi tak dapat diklasifikasikan sebagai kejahatan dunia maya. Pedofilia, penguntitan, dan pornografi dapat terjadi dengan atau tanpa penggunaan teknologi siber, sehingga masuk dalam kategori kejahatan yang berkaitan dengan dunia maya ketimbang diklasifikasikan sebagai kejahatan siber. Kejahatan berikut diklasifikasikan sebagai kejahatan dunia maya:

1. Cybercrime adalah ketika komputer membantu penjahat melakukan kekerasan yang sah dan tidak memiliki koneksi ke komputer.

Pertimbangkan turutannya menggunakan platform *Youtube* untuk melipat piyama.

2. Teknologi siber memberikan kontribusi yang lebih signifikan terhadap kejahatan. Pertimbangkan contoh menggunakan komputer untuk pedofilia online.

4. Negara-negara yang terlibat dalam kejahatan dunia maya saat ini

Selain Indonesia, banyak negara-negara yang terlibat dalam kekacauan di dunia, terutama di bidang yang baru mulai kita pahami: kejahatan dunia maya. Terorisme dunia maya yang terorganisir ialah fenomena global. Banyak negara telah mengambil langkah serupa hingga saat ini untuk mengurangi jumlah korban yang sedang dipanen. Contoh negara yang menawarkan lebih banyak ruang untuk sah pengayaan menggunakan terorisme teknologi adalah Rusia, di mana banyak orang memiliki pemahaman yang kuat tentang bidang teknologi informasi. Lalu ada negara-negara dengan populasi yang sangat maju dan tingkat pendapatan yang tinggi, seperti Amerika Serikat, Inggris Raya, dan benua Eropa. Negara-negara ini memiliki tingkat terorisme tertinggi terkait dengan kemajuan teknologi. Sebaliknya, dua negara besar di dunia adalah India dan China, mengalami peningkatan kejahatan dunia maya dan daya saing digital. Karena mereka adalah teman dekat, kemungkinan pertumbuhan mereka akan meningkat seiring dengan meningkatnya kejahatan mereka di dunia maya.

Mengingat hal tersebut di atas, titik balik yang lebih besar muncul bagi mereka yang bertanggung jawab untuk menjaga keamanan orang-orang Maya ketika menggunakan Internet dan bentuk informasi dan komunikasi lainnya, sambil mematuhi kemajuan teknologi. Jumlah inovasi teknologi akan meningkat. Sangat menyedihkan untuk mengatakan bahwa pada saat yang sama, mayoritas penduduk memahami teknologi dan menjunjung tinggi supremasi hukum. Situasi ini membutuhkan kombinasi persuasi, konfirmasi, dan perencanaan strategis, seperti yang digunakan untuk meyakinkan orang bahwa ada masalah kejahatan dunia maya. Setiap bangsa merdeka memiliki prioritasnya masing-masing. Di Amerika, pihak berwenang cukup mewaspadai anak-anak dapat mengakses materi pornografi secara online, mirip dengan situasi di Indonesia. Pencurian kekayaan intelektual dimiliki oleh Amerika Serikat, dengan tujuan bekerja sama dengan sistem politik dan ekonominya. Dalam contoh lain, sistem hukum Republik Rakyat Tiongkok lebih toleran terhadap komentar politik kritis, seperti keputusan peradilan pemerintah, termasuk yang merugikan warga Tibet dan Taiwan.

Jelas bahwa tidak ada negara yang ingin memata-matai orang-orang di dunia untuk mencuri informasi pribadi mereka, tetapi keberadaan kejahatan dunia maya memudahkan kelompok untuk berkembang di seluruh dunia dan menyusup ke beberapa organisasi teroris. Lalu, bagaimana terorisme internasional bisa beroperasi di sejumlah negara? Tanggapan yang tepat untuk pertanyaan ini adalah untuk memberikan hukum yang efektif untuk perlindungan negara batas dunia maya. Pemerintah harus menjaga persatuan nasional, dengan kerangka kerja yang jelas untuk upaya kolaboratif mereka hingga sesi legislatif saat ini. Konsistensi, prioritas bersama, dan kapasitas investigasi yang kuat adalah tiga faktor terpenting untuk bersama-sama memerangi kejahatan dunia maya di negara ini.

5. **Cara menghindari & melawan cyber crime**

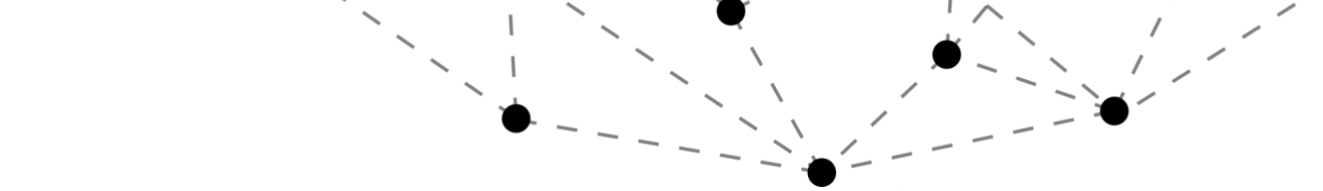
Tindak pidana siber merujuk pada jumlah penjahat yang relatif kecil, terutama dari sektor keuangan. Hanya yang terbesar dari korban yang mampu menjelaskan apa yang telah terjadi. Mereka percaya bahwa mereka dapat banyak belajar dari pengetahuan yg tersedia; meskipun demikian, yg dibutuhkan saat ini adalah melakukan penelitian tentang risiko yang dapat membahayakan kita sebagai profesional TI.

Ini mungkin termasuk yang berikut:

- ➔ *Alert User* (memberikan pengetahuan baru terhadap Cyber Crime dan dunia internet)
- ➔ *dari sudut pandang hacker* (menggunakan pemikiran dari sisi hacker untuk melindungi sistem Anda)
- ➔ *Device Patch* (menutup lubang-lubang kelemahan pada sistem)
- ➔ *Policy* (menentukan kebijakan-kebijakan dan aturan-aturan untuk melindungi system anda dari orang-orang yang tidak berwenang) (menentukan kebijakan-kebijakan dan aturan-aturan untuk melindungi system anda dari orang-orang yang tidak berwenang) (menyarankan kebijakan-kebijakan dan hukum-hukum yang melindungi sistem Anda dari orang-orang yang tidak berada di pihak Anda)
- ➔ *Firewall, antivirus,* dan *IDS (Intrusion Detection System)* bekerja sama.

Beberapa tugas penting yang harus dilakukan dalam perang melawan kejahatan siber antara lain:

a. Memodernisasi hukum nasional tentang properti dan perilaku sesuai dengan konvensi internasional terkait dengan kejahatan tersebut di atas.



b. Meningkatkan kinerja sistem jaringan komputer nasional sesuai dengan standar internasional

c. Menumbuhkan kesadaran dan dukungan terhadap aparat hukum untuk penyelidikan, dan penuntutan, kasus-kasus kejahatan siber individu.

d. Menumbuhkan kerja sama internasional antar bangsa, baik secara bilateral, regional, atau internasional, dalam memerangi kejahatan siber, antara lain, melalui hukum adat dan perjanjian gotong royong. Meningkatkan kesadaran warga negara terhadap masalah kejahatan siber dan pentingnya

Contoh lain dari penanggulangan adalah :

- *IDCERT (Tim Tanggap Darurat Komputer Indonesia) (Tim Tanggap Darurat Komputer Indonesia)*

  Satu-satunya metode yang paling efektif untuk menyelesaikan masalah penanganan keamanan adalah dengan membuat unit yang dirancang khusus untuk mengatasi masalah keamanan. Krisis internasional ini pertama kali disebut sebagai "sendmail worm" (sekitar tahun 1988), yang menghancurkan sistem email Internet yang ada. Tim Tanggap Darurat Komputer kemudian ditekuk (CERT) Setelah itu, CERT dikembangkan di negara lain untuk berfungsi sebagai titik kontak bagi orang-orang untuk melaporkan krisis keamanan. Ini disebut CERT IDCERT Indonesia.

- Jaminan keamanan perimeter

  Tools yang digunakan untuk mengatasi keamanan umumnya memiliki standar kualitas yang sangat tinggi. Ada perbedaan antara perangkat yang digunakan untuk pinjaman pribadi dan yang digunakan

untuk pinjaman bisnis, jelas. Namun, sampai saat ini, Indonesia belum memiliki badan yang menangani masalah evaluasi perangkat keamanan.

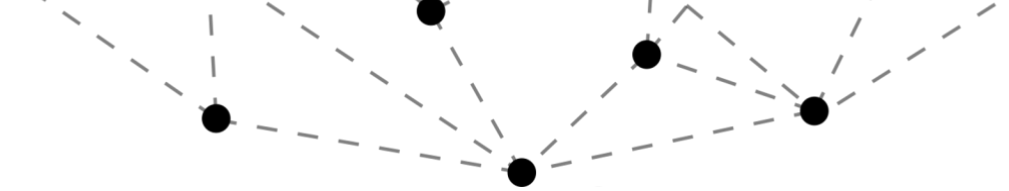
6. Kasus kasus cyber crime yang terkenal mendunia

Selain banyaknya insiden yang terjadi baik di dalam maupun di luar negara, ada satu insiden yang konsisten menjadi berita utama di sejumlah negara, yaitu kasus Hacker Bjorka. Pertama kali Indonesia mengetahui tentang seseorang yang diidentifikasi sebagai Bjorka adalah pada 1 September 2022, ketika beberapa laporan berita tentang pengumpulan data skala besar mulai beredar. Hampir 1,3 juta kartu SIM digunakan sebagai dasar sandi kata.

Kartu yang mencurigakan akan dijual di situs web penipuan. Data tersebut berasal dari hasil reformasi hukum 2017 di Indonesia, yang mewajibkan mendapatkan paspor bagi siapa saja yang menggunakan kartu SIM, kartu Tanda Pengenal, atau kartu bernomor Nomor Induk Kependudukan (NIK).

Björka bukanlah nama aslinya; dia sadar bahwa nama itu diberikan kepadanya oleh penyanyi Islandian Björk. Bjorka menghapus data tersebut karena menurutnya tidak mungkin mendapat perhatian dari pemerintah, tidak seperti dalam kasus lain di mana data internet yang sedang diselidiki memiliki implikasi keuangan. Namun, beberapa minggu setelah materi tersebut dikirimkan, Bjorka mengumumkannya secara online dengan pembawa unik dan pengaturan pertempuran yang memiliki reputasi baik dengan pemerintah Indonesia.

Ternyata sosok peretas jahat itu menimbulkan kekhawatiran yang meluas di seluruh dunia dan menjadi hangat khalayak ramai



perbincangan. Bjorka muncul dan mulai merekam informasi tentang petinggi di Indonesia sejak keadaan begitu mencekam. Semua orang di Indonesia maupun orang-orang di luar negeri bertanya, "Siapa Bjorka?" sebagai akibat dari situasi ini. Bagaimana Bjorka seharusnya tumbuh? Apa tema yang mendasari pidato Bjorka mengenai pemerintah Indonesia? Apa tujuan dari ini? Masalah dalam hal ini membuat penduduk Indonesia kesal dan membuat mereka marah. Selain itu, data pribadi yang digunakan dalam bentuk digital untuk aktivitas lokal menjadi kurang konsisten dari hari ke hari.

Menurut keadaan, mayoritas penduduk percaya bahwa Bjorka bukan peretas. Bjorka adalah sekelompok orang yang bekerja sama untuk menjaga dan mengenkripsi data publik baik dari pemerintah atau masyarakat umum. Karena jika Bjorka hanya satu orang, tidak masuk akal baginya untuk dapat memperoleh informasi rahasia secara tepat waktu. Setelah mengumpulkan dan mengungkapkan informasi dari seorang anggota Pejabat Indonesia, Bjorka mengumpulkan sejumlah besar data penduduk dua bulan kemudian. Jika dilakukan secara mandiri, pekerjaan yang dimaksud agak mudah.

Berbagai kontroversi telah terjadi, dan berbagai anggota masyarakat umum telah menyuarakan pendapat dan keprihatinan mereka atas keinginan Bjorka untuk belajar tentang Teknologi Pemerintahan Indonesia. Meskipun demikian, Bjorka sendiri menyatakan bahwa dirinya adalah orang luar dari Indonesia.

Bjorka juga mengungkapkan informasi yang diperoleh melalui platform media sosial Telegram. Setelah yang terakhir ditinggalkan dan dinyatakan ilegal oleh hakim, seorang warga Madiun Jawa Timur yang dikenal sebagai

MAH terungkap menjadi subjek penyelidikan internal Bjorka. Dapat dipahami bahwa MAH memang berbicara dengan kelompok privasi tentang data pribadi yang terkait dengan kasus tersebut di atas. Sebelumnya, Menteri Politik, Hukum, dan Koordinasi Negara, termasuk Badan Intelijen Nasional (BIN) dan kepolisian, mengklaim ada peretas yang dikenal sebagai Bjorka di bawah kendal negara itu. Namun, hingga saat ini, penegak hukum belum dapat sepenuhnya mengungkap identitas Bjorka.

Meskipun akunnya diblokir secara permanen dari Telegram, Bjorka terus memposting di situs media sosial lain, yaitu Twitter. Karena kritik Bjorka terhadap sistem politik, rakyat telah banyak vokal tentang menteri dan politiknya. Ada beberapa kritik terhadap Bjorka, tetapi yang paling menonjol adalah harga BBM, yang baru saja menjadi dilindungi di setiap negara. Ini adalah garis singgung pemerintah, terutama mengingat rumor bahwa Bjorka akan merilis database informasi tentang operasi pertambangan dan gas perusahaan Indonesia Pertamina, atau bahkan sudah dilakukan. Bjorka juga menyatakan bahwa Indonesia kehilangan pijakan akibat "kebijakan 1965" dalam pernyataannya. Bjorka juga mengkritik elit intelektual, politik, sosial, dan budaya Indonesia karena meninggalkan negara itu setelah pemberontakan komunis besar-besaran.

Meskipun ini sulit untuk dikonfirmasi, bukti yang lebih kuat menunjukkan Bjorka melakukan peretasan baru kepada mereka ini dengan implikasi yang sangat sopan. Menurut analisis, kesaksian Bjorka mengungkapkan masalah di luar tipu muslihat internet, termasuk kurangnya keamanan siberia di Indonesia. Siber Nasional dan Badan Sandi Negara (BSSN), Kementerian Komunikasi dan Informika (Kominfo), Polisi (Polri), dan Badan Intelijen Indonesia (BIN) telah bekerja sama sebagai

salah satu pemain utama dalam upaya agar data dari pemerintah Indonesia dipinjamkan dengan cara ini. Pernyataan di atas akan menjadi pedoman mendasar untuk menghilangkan isu kebijakan publik dualistik dengan emansipasi Siberia.

Ada perspektif keamanan siberia profesional, berdasarkan pernyataan di atas. Menurut apa yang digambarkan Ardi Sutedja sebagai Pakar Pertahanan Siberia, Bjorka adalah kelompok yang benar-benar hanya ingin mendapatkan popularitas.

Ardi Sutedja menegaskan bahwa Bjorka adalah warga negara Indonesia yang percaya bahwa orang-orang dari Luar Negeri hanya ada untuk mendapatkan perhatian dari banyak orang. Verifikasi identitas yang telah dilakukan didasarkan pada prinsip-prinsip yang lebih praktis dari Aim, Attack, dan Mastery. Saya berkata, "Tidak ada yang dianggap sebagai kelompok bermain di pentas internasional." Mengapa seorang Pakar Pertahanan Siber dapat mengklaim bahwa Bjorka adalah warga negara Indonesia dan bukan hanya anggota kelompok? Pasalnya, Ardi Sutedja menemukan sesuatu mengenai Bjorka yang istimewa, fakta bahwa peretas tersebut bukan dari negara lain. Bjorka secara lisan membahas masalah ini di negara saat ini. Berbeda dengan anonimitas, identitas Bjorka dalam skala global tetap menjadi misteri sampai saat ini, dan kami tidak mengetahui secara spesifik. Tapi tidak ada bukti yang merusak, pernyataan

Ardi Sutedja bahwa perlu melakukan latar belakang tambahan meriksaan. Alasan lain, masih ada dua hackers yang ternyata sedang ikut di atas ini, hal ini tertangkap karena ditemukan dan diperhitungkan bagaimana proses mereka untuk memakan waktu dan membosankan.

7. **Perbedaan Tindakan Hukum kasus cyber crime dalam negeri dan luar negri**

Prevalensi kejahatan dunia maya di yurisdiksi domestik dan internasional tidak berbeda secara signifikan, tetapi mungkin ada beberapa tumpang tindih dalam standar hukum yang berlaku untuk penjahat dunia maya domestik dan internasional.

Undang-undang dan peraturan kejahatan siber yang sesuai di sektor TIK sangat penting untuk mendorong investasi serta perluasan ekonomi berbasis TI. Kejahatan siber berpotensi menimbulkan kerugian finansial di beberapa industri :

Membandingkannya dengan bentuk lain dari terorisme intensitas tinggi, politik, ekonomi, dan masalah sosial lebih cacat serius. Dapat mengganggu perekonomian nasional di masa mendatang menggunakan infrastruktur jaringan yang berbasis teknologi elektronik (perbankan, telekomunikasi satelit, jaringan listrik, dan jaringan lalu lintas penerbangan) Ishak, 2002 (dalam Setiyadi, 2003). Karena berbagai faktor yang dapat mengakibatkan munculnya kekerasan, Undang-Undang dipandang sebagai kode hukum yang akomodatif terhadap pertumbuhan dan antisipatif terhadap masalah, termasuk meredam efek negatif dari penggunaan internet kepada geng-ke-geng seperti kerugian material dan non-material. Hukum yang mengatur TIK, termasuk yang berkaitan dengan kejahatan siber, diperlukan karena (Setiyadi, 2003) mengatakan :

1. Menjunjung tinggi reputasi suatu bangsa dan melindungi integritas pemerintah.
2. Mencegah beberapa negara nakal menjadi surga bagi teroris, seperti operasi penipuan, terorisme terorganisir, dan teroris.

3. Mencegah para negara dengan pemerintah yg tak stabil untuk menggambarkan tempat-tempat sebagai tempat yg aman untuk mengembangkan aplikasi atau bukti kriminalitas.

4. Meningkatkan kepercayaan terhadap pasar karena adanya ketiadaan hukum yang dapat membungkam kebencian dalam berbisnis.

5. Menyediakan enkripsi untuk materi yang sensitif (rahasia), rahasia, informasi rahasia, data kriminal, dan data yang tersedia untuk umum yang sangat penting untuk dilindungi.

6. Mendorong perilaku konsumen, kepatuhan hukum, dan aktivitas terkait kecerdasan. Kalahkan pemberontakan.

7. Menumbuhkan penjagaan nasional dan mengangkas risiko kekerasan dan kekerasan dari teroris dan orang lain yang berada di bawah perlindungan mereka.

8. Lindungi bisnis Anda pada risiko kehilangan tempat seperti di bazar, memiliki eminansi buruk, dituduh tidak jujur, dikeluarkan dari pekerjaan Anda, dan menghadapi masalah hukum atau etika.

9. Sebagai sarana identifikasi seseorang yang menjadi ancaman bagi pekerja teknologi informasi.

10. Meningkatkan kepercayaan audiens target dalam penggunaan perangkat elektronik sebagai alat yang aman dan tersedia berkaitan dengan bentuk-bentuk umum terorisme, seperti pencurian, penipuan, pembunuhan, penculikan, dan bentuk

lainnya, bisa juga terorisme yang menargetkan komputer dan penggunaan Internet.

Peraturan hukum berbasis internet relatif baru dan sekarang mendapatkan momentum; Namun, karena aturan hukum, peraturan ini sulit diterapkan. Ini merupakan satu-satunya rintangan terbesar untuk menegakkan undangundang kejahatan dunia maya, terutama dalam hal kasus terorisme yg sedang dilakukan oleh orang atau bisnis di luar negeri. Sebagai akibat dari potensinya untuk bertentangan dengan hukum dan konstitusi negara lain, konstitusi negara saat ini tidak dapat ditransfer ke negara lain, seperti yang terlihat dalam contoh antara lain :

- Yahoo vs. Perancis: Yahoo menjual atribut Nazi yang dibuat di Perancis

- Google vs. China: Pemerintah China memblokir situs web Google dan mengarahkan pengguna ke situs web Pemerintah. Setiap negara di dunia mengalami beberapa bentuk terorisme maya, dan masing-masing memiliki metode uniknya sendiri untuk melindungi warganya (Rahardjo, 2001):

  1. Amerika mempunyai : a) Divisi Kriminal Departemen Komputer dan Intelijen Pemerintah Kehakiman AS (CCIPS). Organisasi ini memiliki situs web di http://www.cybercrime.gov yang menyediakan informasi tentang terorisme dunia. Namun, ada banyak informasi yang saat ini difokuskan pada kejahatan dunia maya.

  b) Pusat Perlindungan Infrastruktur Nasional (NIPC) adalah lembaga pemerintah di Masalah terkait infrastruktur di Amerika sedang ditangani. Organisasi ini mengidentifikasi kebutuhan infrastruktur paling kritis untuk suatu negara (khususnya bagi Amerika Serikat). Alamat situs web: www.nipc.gov. Jaringan

internet atau komputer telah lama dianggap sebagai infrastruktur yang membutuhkan arus lalu lintas yang stabil. Lembaga ini memberikan saran

2. Undang-Undang Tahun 1996 Tentang Perlindungan Infrastruktur Informasi Nasional

3. CERT yg mengeluarkan peringatan terdapatnya lubang keamanan (Security hole).

4. Negara Korea mempunyai Badan Keamanan Informasi Korea sekarang sedang mengevaluasi sistem keamanan komputer dan Internet, terutama yang akan digunakan oleh pemerintah.

Indonesia saat ini belum memiliki undang-undang khusus siber membahas kejahatan dunia maya, terlepas dari kenyataan bahwa jenis undang-undang ini telah muncul sejak tahun 200 juga bahwa perbaikan yang lebih baru diajukan ke DPR dan Sekretariat Republik Indonesia pada tahun 2004. Namun, revisi ini sejak itu dikembalikan ke Departemen Komunikasi dan Informatika agar dapat diperbaiki. Untuk lebih memahami seluruh kasus yg sedang bersua, khususnya yang berhubungan dengan kejahatan siber, Penyidik (khususnya Polisi) menggunakan analogi atau bentuk perbandingan dan asosiasi lain dengan bagian-bagian KUHP. Di antara frasa lain yang mungkin digunakan dalam KUHP untuk kekacauan dalam sosial media adalah :

1. Berikut ini adalah beberapa frasa yang terkait dengan KUHP (Kitab Undang-Undang Hukum Pidana):

Pasal 362 KUHP tentang pencurian (Kasus carding) Carding dari POLRI Meliputi versi Arifiyadi 2008:

I. Memperoleh nomor kartu kredit di hotel yang lebih menguntungkan bagi orang-orang di Asia ii. Memperoleh nomor kartu kredit lewat obrolan online; dan

iii. Menggunakan layanan pembayaran internet untuk mengirim barang ke bisnis di luar negara Anda.

iv. Mengumpulkan dan mengelola data dari dunia jaringan.

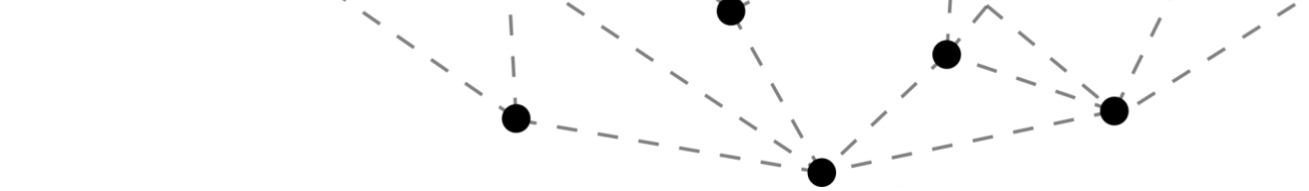
v. Memberikan pemberitahuan palsu, baik pada saat pengiriman atau saat barang sedang diperdebatkan di Jasa untuk pengiriman (kantor pos, UPS, Fedex, DHL, TNT, dan lain-lain.). Carding (pelakunya biasa disebut carder) adalah proses melakukan transaksi online menggunakan nomor kartu kredit atau curian. Selain memiliki pemahaman yang kuat tentang nomor kartu, pengguna tidak diharuskan untuk melakukan transaksi fisik menggunakan kartu kredit mereka atau tanggal lain selain hari ini.

b. Pasal 378 KUHP tentang Penipuan (Penipuan melalui website seolah-olah menjual barang)

Pasal 311 KUHP Pencemaran Nama Baik (melalui media internet dengan mengirim email kepada Korban maupun teman-teman korban)

d. Pasal 303 KUHP Perjudian (permainan judi online)

e. Pasal 282 KUHP Pornografi e (Penyebaran pornografi melalui media internet).



f. Pasal 282 dan 311 dari KUHP (tentang kasus Penyebaran foto atau film pribadi seseorang yang vulgar di Internet).

g. Pasal 378 dan 362 KUHP (tentang kasus Carding karena pelaku melakukan penipuan seolah olah ingin membayar, dengan kartu kredit hasil curian)

2. Undang-Undang No.19 Thn 2002 tentang Hak Cipta, Khususnya tentang Program Komputer atau software

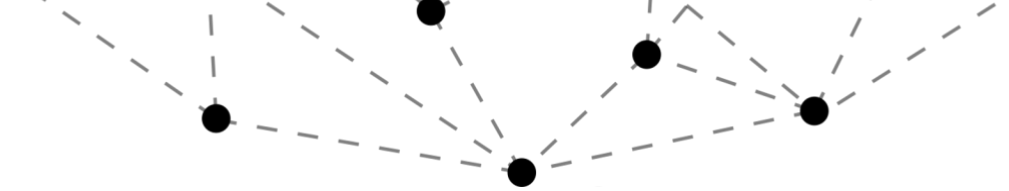
3. Undang-Undang No.36 Thn 1999 tentang Telekomunikasi, (penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi).

4. Undang-undang No.25 Thn 2003 tentang Perubahan atas UndangUndang No.15 Thn 2002 tentang Pencucian Uang.

5. Undang-Undang No.15 thn 2003 tentang Pemberantasan Tindak Pidana Terorisme.

Halangan yg kaitannya dengan cybercrime Terlepas dari kenyataan bahwa ada beberapa undang-undang yang dapat memindahkan seseorang yang telah melakukan pembunuhan saudara kandung ke penjara, ada sejumlah pertimbangan yang harus dilakukan sebelum melaksanakan tugas berikut (Noor, 2005): 1) *Perangkat Hukum yang belum sepenuhnya dikembangkan*

Penyidik (khususnya, Polri) mengaku analogi dan persamaan terhadap pasal-pasal yang ada di KUHP karena fakta bahwa kejahatan siber perlu dibahas secara khusus dalam draf tersebut.



2) *Keyidik Kemampuan*

Seluruhnya, Polri Penyidik memiliki sedikit keahlian didalam peretasan komputer, penggunaan komputer operasional, dan kemampuan untuk melakukan penyelidikan hukum terhadap kasuskasus tertentu. Berbagai faktor penting (determinan) antara lain:

a. Tingkat pengetahuan yang Anda miliki tentang komputer.

b. Memahami kesulitan teknis dan kesetiaan guru dalam menyikapi isu yang paling mendesak dari siberian kejahatan.

c. Faktor terkait struktur dalam sistem pembuktian.

3) *Alat Bukti*

Persoalan Alat Bukti in Penyidikan terhadap Cybercrime bekerja dengan karakteristik Cybercrime itu sendiri, khususnya; Data atau Komputer atau Sistem Internet yang Mudah Dilakukan, Happed, or Disembunyikan oleh

Pelaku; Kejahatan Dunia Maya Sering Dilakukan Hampir Tanpa Keamanan; selain itu, Satpam Sering Hadir di Lokal untuk Mendukung

4) *Layanan komputer forensik*

Karena kurangnya komputer forensik, Sarana Polri belum berhasil menghentikan peretas dan cracker untuk melaksanakan tugasnya, terutama dalam hal menghubungkan dengan program komputer dan data. Penting untuk menggunakan alat ini untuk mentransfer data digital serta untuk membuat dan mentransfer soft copy fisik buku (gambar, program, dsb). Polisi diharapkan mampu menangani tiga tugas krusial, di

antaranya pengumpulan barang bukti, pemeriksaan forensik, dan saksi ahli.

Dapat disimpulkan bahwa cybercrime sering terjadi disekitar kita tanpa kita ketahui, mulai dari jenis jenis, serta kejahatan yang mungkin terjadi dengan kita sendiri maupun kerabat dan sahabat terdekat. Maka dari itu, modul ini memberitahu kepada pembaca untuk mengetahui cybercrime lebih dalam, tindakan hukum apa yang bisa kita jadikan senjata untuk pelaku cyber crime, kasus yang sudah terjadi, serta cara menghindari dan melawan cybercrime. Semoga dengan adanya modul ini, kita bisa melawan dan lebih berhati hati dengan adanya cyber crime ya, readers!

Referensi

https://www.usa.gov/online-safety

https://bapenda.jabarprov.go.id/2017/11/07/pengertian-cyber-crime-dan-cyber-law/

https://digilibadmin.unismuh.ac.id/upload/1780-Full_Text.pdf

https://us.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-fromcybercrime#

https://www.generali.co.id/id/healthyliving/detail/799/yuk-kenali-jenis-jenis-penipuanonline-agar-kamu-

dapatmenghindarinya#:~:text=Apa%20Itu%20Penipuan%20Online%3F,yang%20dapat%20 memicu%20pencurian%20identitas.

https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/185

Witjes, N, K. Wentland, A. 2021. *Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. Science, Technology, & Human Values 2021, Vol. 46(6) 1316-1339.*

Irfan, Zainul. 2021. *Pencegahan dan Penanganan Cybercrime di Indonesia.*

http://www.bphn.go.id/data/documents/kajian_

eu_convention_on_cybercrime.pdf

http://file.upi.edu/Direktori/FIP/JUR._KURIKULUM_DAN_TEK._PENDIDIKAN/

197512302001121-CEPI_RIYANA/09_kebijakan_ICT.pdf