Fujiama Diapoldo Silalahi S.Kom, M.Kom

KEAMANAN SIBER (CYBER SECURITY)

YAYASAN PRIMA AGUS TEKNIK

KEAMANAN CYBER (CYBER SECURITY)

Penulis :
Fujiama Diapoldo Silalahi, S.Kom, M.Kom.

ISBN : 9 786235 734811

Editor :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds.,M.Kom.

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : info@stekom.ac.id

KATA PENGANTAR

Puji syukur pada Tuhan Yang Maha Esa bahwa buku yang berjudul "***Keamanan Siber (Cyber Security)***" ini dapat diselesaikan dengan baik. *Cyber security* (Keamanan Siber) merupakan suatu aktivitas dengan maksud untuk melindungi perangkat komputer, perangkat *mobile*, server, sistem elektronik, jaringan, dan data dari beraneka jenis serangan jahat digital. Serangan jahat digital itu biasa dikenal dengan sebutan *cyber attack.* Dampak dari *cyber attack* salah satunya yaitu kerugian global. Contohnya pada kasus *WannaCry* yang sempat mengacaukan dunia beberapa tahun lalu, *WannaCry* telah menginfeksi setidaknya 230.000 perangkat di 150 negara yang mengakibatkan kerugian kurang lebih US$4 Miliyar secara global. Cara yang biasa digunakan sebuah organisasi atau perusahaan untuk meminimalisir ancaman terhadap *cyber security* yakni dengan menerapkan standar *cyber security.* Standar cyber security yang paling banyak dikenal saat ini adalah ISO/IEC 27001, NIST Cybersecurity Framework, dan PCI DSS. ISO/IEC 27001 pertama kali diterbitkan di tahun 2005 oleh ISO yang merupakan badan yang mengelola standar internasional dan IEC (International Electrotechnical Commission) yang mengelola standar untuk elektronik. NIST (National Institute of Standards and Technology) Cybersecurity Framework pertama kali diterbitkan pada tahun 2014 yang merupakan standar *cyber security* untuk organisasi swasta di Amerika Serikat yang pada awalnya hanya ditujukan untuk mengoperasikan infrastruktur vital seperti air dan listrik, namun sekarang sudah banyak digunakan oleh sejumlah negara lain. PCI DSS (Payment Card Industry Data Security Standard) pertama kali diterbitkan di tahun 2004 yang merupakan standar *cyber security* untuk organisasi yang mengurusi kartu pembayaran seperti kartu kredit.

Jenis serangan siber (*cyber attack*) seiring waktu terus mengalami peningkatan, namun sayangnya masih banyak pebisnis yang kurang paham akan pentingnya *cyber security.* Tanpa tata cara keamanan yang kuat, tanpa disadari kegiatan bisnis bisa dilacak oleh pelaku kejahatan digital. Buku ini menyajikan berbagai pokok pembahasan seputar *cyber security* seperti perang siber mengenai pencurian identitas, masalah privasi dan sekuritas online, pedoman aksesibilitas konten web, peran organisasi international terhadap kejahatan digital dan sebagainya. disajikan mulai dari teori sampai studi kasus tentang *cyber security.* Penulis berharap buku ini bisa memberikan manfaat dan pandangan baru baik hanya sekedar untuk pengetahuan atau mengimplementasikanya dilapangan. Akhir kata penulis ucapkan terima kasih.

Semarang, Agustus 2022
Penulis

Fujiama Diapoldo Silalahi S.Kom, M.Kom

DAFTAR ISI

BAB 1
KEAMANAN DAN MANAJEMEN DATA

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan Keamanan dan Pengelolaan Data
- Memahami upaya internasional dengan mengacu pada Keamanan dan Manajemen Data
- Memahami masalah teknis dan hukum terkait Keamanan dan Manajemen Data

1.1 PENGANTAR

Keamanan komputer adalah masalah yang tidak terpecahkan. Jadi, alih-alih mencoba menyelesaikannya, perusahaan harus memikirkan keamanan jaringan sebagai serangkaian risiko yang melekat dalam melakukan bisnis online. Melihat keamanan dari perspektif itu akan menghasilkan keputusan yang lebih baik dan desain teknologi yang unggul. Jelas, keamanan menimbulkan beberapa masalah langsung, dan bisnis harus memeriksa apakah mereka telah menyelesaikannya. Pengungkapan baru-baru ini bahwa protokol pembayaran di beberapa situs e-commerce yang banyak digunakan memungkinkan pelanggan untuk membeli bahkan barang fisik tanpa membayar adalah contoh masalah keamanan yang dapat diukur dan dipecahkan. Tetapi lebih sering, keamanan komputer lebih baik ditangani dengan pendekatan manajemen risiko, yang tidak memerlukan kuantifikasi yang tepat. Ini adalah masalah personalia — seperti konflik kantor, pencurian kecil-kecilan, salah mengartikan kredensial karyawan, dan kesehatan karyawan. Pertimbangkan bahwa karyawan yang mengambil risiko untuk menyelesaikan pekerjaan mereka adalah aset bagi organisasi dan ancaman terhadap keamanan komputer. Misalnya, seorang karyawan yang berhasil melakukan tunnel di sekitar firewall perusahaan untuk login dari jarak jauh melihat hasil positif dari akses dari rumah. Atasan karyawan hanya melihat peningkatan produktivitas. Risiko keamanan adalah bagian dari menyelesaikan pekerjaan. Jaringan dan konektivitas secara inheren termasuk risiko seperti mempekerjakan manusia secara inheren membawa risiko.

1.2 APA ITU KEAMANAN DATA?

Keamanan data mengacu pada langkah-langkah perlindungan privasi digital yang diterapkan untuk mencegah akses tidak sah ke komputer, database, dan situs web. Keamanan data juga melindungi data dari korupsi. Keamanan data adalah prioritas utama bagi organisasi dari berbagai ukuran dan genre. Keamanan data juga dikenal sebagai keamanan informasi (IS) atau keamanan komputer. Contoh teknologi keamanan data mencakup enkripsi disk perangkat lunak/perangkat keras, pencadangan, penyamaran data, dan penghapusan data.

Ukuran teknologi keamanan data utama adalah pengacakan, di mana data digital, perangkat lunak/perangkat keras, dan hard drive diacak dan dibuat tidak dapat dibaca oleh pengguna dan peretas yang tidak berwenang. Keamanan data juga sangat penting untuk catatan perawatan kesehatan, sehingga advokat kesehatan dan praktisi medis di AS dan

negara lain berupaya menerapkan privasi catatan medis elektronik (EMR) dengan menciptakan kesadaran tentang hak pasien terkait dengan pelepasan data ke laboratorium, dokter , rumah sakit dan fasilitas kesehatan lainnya.

Keamanan dan privasi data memberikan perlindungan data di seluruh perusahaan. Bersama-sama, mereka terdiri dari orang-orang, proses dan teknologi yang diperlukan untuk mencegah kekuatan destruktif dan tindakan yang tidak diinginkan. Keamanan dan privasi data bukanlah hal yang baik untuk dimiliki. Mereka diwajibkan oleh lebih dari 50 mandat hukum dan industri internasional, serta para pemimpin bisnis. Dengan 2,5 triliun byte data yang dibuat setiap hari, dan dengan biaya rata-rata insiden terkait keamanan di era data besar diperkirakan lebih dari USD40 juta, sekaranglah saatnya untuk menjaga informasi identitas pribadi (PII) pelanggan, bisnis, dan jenis data sensitif lainnya yang aman dari ancaman internal dan eksternal. Data harus dilindungi di mana pun ia berada—dalam basis data, aplikasi, atau laporan di seluruh lingkungan produksi dan non-produksi. Data adalah bentuk mentah dari informasi yang disimpan sebagai kolom dan baris dalam database, server jaringan, dan komputer pribadi kami. Ini mungkin berbagai informasi dari file pribadi dan kekayaan intelektual hingga analisis pasar dan detail yang dimaksudkan untuk sangat dirahasiakan. Data bisa berupa apa saja yang menarik yang dapat dibaca atau ditafsirkan dalam bentuk manusia.

Namun, beberapa informasi ini tidak dimaksudkan untuk keluar dari sistem. Akses tidak sah dari data ini dapat menyebabkan banyak masalah bagi perusahaan yang lebih besar atau bahkan pengguna rumahan pribadi. Mencuri detail rekening bank Anda sama merusaknya dengan administrator sistem yang baru saja dirampok untuk mendapatkan informasi klien di database mereka. Ada penekanan besar pada keamanan data akhir-akhir ini, terutama karena internet. Ada sejumlah opsi untuk mengunci data Anda dari solusi perangkat lunak hingga mekanisme perangkat keras. Pengguna komputer tentu lebih sadar akhir-akhir ini, tetapi apakah data Anda benar-benar aman? Jika Anda tidak mengikuti panduan penting, informasi sensitif Anda mungkin berisiko.

1.3 MELINDUNGI DATA SENSITIF

Era Informasi telah membawa serta kemampuan untuk berbagi, menyimpan, dan mengirimkan data dengan mengklik mouse. Bagian yang berisiko dari persamaan ini adalah bahwa penyimpanan dan transmisi data sensitif di seluruh sistem komputer mungkin sulit untuk dilindungi, sehingga meningkatkan kebutuhan akan kewaspadaan. Di dunia kertas, jika sebuah dokumen bertanda "KLASIFIKASI" atau "RAHASIA", kita dapat dengan mudah melindunginya dengan meletakkannya menghadap ke bawah di meja kita ketika seseorang lewat yang tidak perlu tahu, menguncinya di lemari arsip saat tidak digunakan, atau ketika perlu berbagi gunakan kurir atau antar ke orang yang tepat, dan akhirnya ketika tidak diperlukan lagi kami dapat mencabik-cabiknya. Kita perlu mengambil tindakan pencegahan yang sama di dunia komputer. Sistem komputer itu kompleks. Mereka dapat mencakup perangkat lunak sistem operasi, aplikasi dan program, database, komponen perangkat keras, dan jaringan. Masing-masing elemen ini memerlukan metode yang berbeda untuk melindungi data. Menambah kompleksitas adalah dinamisme dalam hal cara sistem dan bagian-bagiannya berinteraksi dan persyaratan mereka untuk sering memperbarui untuk memperbaiki bug atau melindungi dari serangan peretasan terbaru. Semua ini secara kolektif menggarisbawahi

perlunya kita masing-masing untuk bertanggung jawab melindungi data sensitif yang kita tangani. OIT hadir untuk membantu, jika Anda memiliki pertanyaan tentang keamanan sistem atau dokumen elektronik yang Anda tangani. Secara umum, profesional Keamanan Informasi menyarankan bahwa melindungi data sensitif memerlukan kombinasi orang, proses, kebijakan, dan teknologi.

1.4 DATA SENSITIF PERAMBAN

Kembali di musim panas 2013 Google dikritik karena menyimpan nama pengguna dan kata sandi informasi login pengguna dalam teks biasa di browser web tanpa perlindungan apa pun. Bagi sebagian orang, ini adalah risiko keamanan kritis yang dapat dengan mudah dihindari, misalnya dengan menerapkan kata sandi utama yang melindungi data. Lainnya dan Google menunjukkan bahwa akses lokal diperlukan untuk mengakses data, dan jika akses lokal diberikan, komputer tetap dikompromikan membuka vektor serangan lain juga. Beberapa hari yang lalu, perusahaan riset keamanan Identity Finder, menemukan masalah terkait lainnya di Google Chrome. Menurut temuan perusahaan, Chrome menyimpan informasi sensitif, yang dimasukkan di situs web dan layanan https, dalam teks biasa di cache browser. Sementara banyak yang percaya bahwa browser tidak menyimpan halaman dan data https karena sifat koneksi yang aman, perlu dicatat bahwa konten https dapat di-cache. Ini hanya bergantung pada header respons situs atau server (yang ditransfer ke browser web). Jika header caching mengizinkan caching konten HTTPS, browser web akan melakukannya.

Chrome dan data sensitif: Pencari Identitas menemukan bahwa Chrome menyimpan berbagai informasi sensitif dalam cache-nya termasuk nomor rekening bank, nomor kartu kredit, nomor jaminan sosial, nomor telepon, alamat surat, email, dan lainnya. Perusahaan mengkonfirmasi bahwa informasi ini dimasukkan di situs web yang aman, dan dapat dengan mudah diekstraksi dari cache dengan program pencarian yang memindai semua jenis file untuk data teks biasa. Data tidak dilindungi dalam cache, yang berarti bahwa siapa pun yang memiliki akses ke data tersebut dapat mengekstrak informasi tersebut. Ini tidak berarti akses lokal, karena perangkat lunak berbahaya yang berjalan di komputer pengguna, dan bahkan rekayasa sosial, dapat memberikan hasil yang sama. Menyerahkan komputer ke bengkel komputer, mengirimkannya ke produsen, atau menjualnya di eBay atau Craigslist dapat memberi pihak ketiga akses ke informasi sensitif yang disimpan oleh browser.

Bagaimana Anda bisa melindungi data Anda dari ini? Google ingin Anda menggunakan enkripsi disk penuh di komputer Anda. Sementara itu menangani masalah akses lokal, itu tidak akan melakukan apa pun terhadap serangan malware atau rekayasa sosial. Ini seperti mengatakan bahwa operator situs web dapat menyimpan kata sandi dalam teks biasa di database, karena pertempuran tetap akan hilang jika seseorang memperoleh akses ke server secara lokal atau jarak jauh. Berkenaan dengan Chrome, satu-satunya opsi yang Anda miliki adalah menghapus cache, mengisi data formulir secara otomatis, dan riwayat penelusuran secara teratur dan sebaiknya segera setelah Anda memasukkan informasi sensitif di browser. Anda tidak dapat mengotomatiskan proses menggunakan Chrome saja, tetapi memerlukan alat atau ekstensi pihak ketiga untuk menghapus data saat Anda menutup browser secara otomatis.

Peramban lain: Pencari Identitas hanya menganalisis cache Google Chrome dan jika Anda tidak menggunakan peramban, Anda mungkin bertanya-tanya apakah peramban Anda juga menyimpan informasi sensitif dalam teks biasa. Firefox, yang maha kuasa dalam hal menyesuaikan browser, memungkinkan Anda menonaktifkan cache SSL dalam konfigurasi lanjutan.

- Ketik about: config di address bar dan tekan enter.
- Konfirmasikan bahwa Anda akan berhati-hati jika ini adalah kunjungan pertama Anda ke halaman tersebut.
- Cari browser.cache.disk_cache_ssl
- Setel preferensi ke false dengan klik dua kali pada namanya untuk menonaktifkan cache SSL.
- Ulangi proses tersebut jika Anda ingin mengaktifkannya kembali.

Firefox akan menggunakan memori komputer untuk menyimpan file, yang berarti bahwa informasi tersebut secara otomatis dihapus ketika Firefox ditutup, dan tidak pernah direkam ke disk.

1.5 TATA KELOLA DATA

Tata kelola data (DG) mengacu pada manajemen keseluruhan ketersediaan, kegunaan, integritas, dan keamanan data yang digunakan dalam suatu perusahaan. Program tata kelola data yang baik mencakup badan atau dewan pengatur, seperangkat prosedur yang ditentukan, dan rencana untuk melaksanakan prosedur tersebut. Langkah awal dalam implementasi program tata kelola data melibatkan penentuan pemilik atau penjaga aset data di perusahaan.

Kebijakan harus dikembangkan yang menentukan siapa yang bertanggung jawab atas berbagai bagian atau aspek data, termasuk akurasi, aksesibilitas, konsistensi, kelengkapan, dan pemutakhirannya. Proses harus didefinisikan mengenai bagaimana data disimpan, diarsipkan, dicadangkan, dan dilindungi dari kecelakaan, pencurian, atau serangan. Serangkaian standar dan prosedur harus dikembangkan yang mendefinisikan bagaimana data akan digunakan oleh personel yang berwenang. Terakhir, serangkaian kontrol dan prosedur audit harus diterapkan untuk memastikan kepatuhan berkelanjutan terhadap peraturan pemerintah.

Area Fokus untuk Tata Kelola Data: Fokus pada Kualitas Data: Jenis program ini biasanya muncul karena masalah seputar kualitas, integritas, atau kegunaan data. Ini mungkin disponsori oleh grup Kualitas Data atau tim bisnis yang membutuhkan data dengan kualitas lebih baik. (Misalnya: Akuisisi Data atau Merger & Akuisisi.). Jenis program ini hampir selalu melibatkan perangkat lunak Kualitas Data, yang dapat digunakan oleh staf bisnis, staf teknis, Petugas Data, tim Tata Kelola Data, atau lainnya. Jenis program ini dapat dimulai dengan fokus perusahaan, atau upaya mungkin bersifat lokal untuk departemen atau proyek. Kadang-kadang, mo]b aip_lh[h]_ aliojm [^ijn nb_ jbifimijbs i` []n fi][f, \on nbihe afi\[f' mi program akan siap untuk diskalakan jika kelompok lain di perusahaan menginginkannya untuk menuai manfaat yang disadari oleh pengadopsi awal.

Jenis data apa yang biasanya ditangani oleh program tersebut pada iterasi awal program?

- Kumpulan Data Master
- Data sensitif
- Data yang Diperoleh
- Data kepentingan kelompok pemangku kepentingan

Piagam untuk jenis program ini dapat membuat peserta Tata Kelola Data dan Penatagunaan bertanggung jawab untuk:

- Tetapkan arah untuk Kualitas Data
- Kumpulkan aturan Kualitas Data dari seluruh organisasi ke dalam satu set yang dapat diakses oleh pemangku kepentingan, Data Stewards, dan peserta Tata Kelola Data lainnya
- Rekonsiliasi kesenjangan, tumpang tindih, dan inkonsistensi dalam aturan Kualitas Data
- Memantau Kualitas Data
- Melaporkan status untuk inisiatif yang berfokus pada kualitas
- Mengidentifikasi pemangku kepentingan, menetapkan hak keputusan, memperjelas akuntabilitas

Semua program Tata Kelola Data tidak sama. Justru sebaliknya: program dapat menggunakan kerangka kerja yang sama, menggunakan proses yang sama, dan masih tampak sangat berbeda.

Kenapa ini? Itu karena organisasi mencoba membuat keputusan tentang atau menegakkan aturan. Organisasi yang peduli dengan Privasi atau Kepatuhan Data akan melihat datanya secara berbeda dari organisasi yang peduli tentang penerapan Gudang Data baru.

Di bagian ini, kami melihat program Tata Kelola Data dengan enam area fokus umum. Tidak ada artinya: Kerangka tunggal dapat membantu mengatur upaya untuk semua area fokus ini karena kesamaan dari semua program Tata Kelola Data:

- Mereka semua memiliki aktivitas yang membahas misi tata kelola tiga bagian: membuat aturan, menyelesaikan konflik, dan menyediakan layanan berkelanjutan.
- Mereka semua menggunakan sebagian besar atau semua komponen universal dari program Tata Kelola Data.
- Semuanya membahas proses dan layanan tata kelola universal, seperti Penyelesaian Masalah dan Kepedulian Pemangku Kepentingan.

Namun, program Tata Kelola Data dengan area fokus berbeda akan berbeda dalam jenis aturan dan masalah yang akan mereka tangani. Mereka akan berbeda dalam penekanan yang mereka berikan pada keputusan dan tindakan terkait tanggal tertentu. Dan, mereka akan berbeda dalam tingkat keterlibatan yang diperlukan dari jenis pemangku kepentingan data.

Siapa pemangku kepentingan data?: Setiap individu atau kelompok yang dapat mempengaruhi atau dipengaruhi oleh data yang sedang dibahas. Beberapa pemangku kepentingan jelas – kelompok bisnis, tim TI, Arsitek Data, dan DBA. Pemangku kepentingan lain mungkin tidak begitu jelas untuk keputusan atau situasi tertentu. Mengetahui pemangku kepentingan mana yang akan dibawa ke meja – dan kapan – adalah tanggung jawab tim Tata Kelola Data.

Area Fokus untuk Tata Kelola Data: Fokus pada Privasi / Kepatuhan / Keamanan: Jenis program ini biasanya muncul karena kekhawatiran tentang kontrol atau kepatuhan Keamanan

Informasi Data. Kepatuhan, dalam konteks ini, dapat merujuk pada kepatuhan terhadap peraturan, kepatuhan kontrak, atau kepatuhan terhadap persyaratan internal. Fokus ini sering terlihat digabungkan dengan fokus pada penegakan kebijakan. Itu juga terlihat dikombinasikan dengan fokus pada Kualitas Data.

Program ini hampir selalu merupakan hasil dari mandat manajemen senior. Ini mungkin secara resmi disponsori oleh Bisnis atau TI, atau mungkin merupakan hasil dari program Tata Kelola, Risiko, dan Kepatuhan (GRC). Program-program ini umumnya dimulai dengan lingkup perusahaan, tetapi seringkali upaya terbatas pada jenis data tertentu. Mereka hampir selalu menyertakan teknologi untuk menemukan data sensitif, untuk melindungi data, dan/atau untuk mengelola kebijakan atau kontrol.

Piagam untuk jenis program ini dapat membuat peserta Tata Kelola Data dan Penatagunaan bertanggung jawab untuk:

- Membantu menemukan data sensitif di seluruh sistem
- Menyelaraskan kerangka kerja dan inisiatif tata kelola, kepatuhan, keamanan, dan teknologi
- Membantu menilai risiko dan menentukan kontrol terkait data untuk mengelola risiko
- Membantu menegakkan peraturan, kontrak, persyaratan kepatuhan arsitektur
- Dukungan Manajemen Akses dan Persyaratan Keamanan
- Mengidentifikasi pemangku kepentingan, menetapkan hak keputusan, memperjelas akuntabilitas

1.6 INTERNET EXPLORER DAN KEAMANAN JARINGAN

Rekomendasi keamanan jaringan umum- Berikut ini adalah panduan keamanan umum untuk semua jaringan rumah dan kantor kecil:

Selalu perbarui komputer Anda: Untuk membantu menjaga komputer di jaringan Anda lebih aman, aktifkan pembaruan otomatis di setiap komputer. Windows dapat secara otomatis menginstal tanggal penting dan yang direkomendasikan, atau pembaruan penting saja. Pembaruan penting memberikan manfaat yang signifikan, seperti peningkatan keamanan dan keandalan. Pembaruan yang disarankan dapat mengatasi masalah yang tidak kritis dan membantu meningkatkan pengalaman komputasi Anda. Pembaruan opsional tidak diunduh atau diinstal secara otomatis.

Gunakan firewall: Firewall dapat membantu mencegah peretas atau perangkat lunak berbahaya (seperti worm) mendapatkan akses ke komputer Anda melalui jaringan atau Internet. Firewall juga dapat membantu menghentikan komputer Anda mengirim perangkat lunak berbahaya ke komputer lain.

Jalankan perangkat lunak antivirus di setiap komputer: Firewall membantu mencegah worm dan peretas, tetapi tidak dirancang untuk melindungi dari virus, jadi Anda harus menginstal dan menggunakan perangkat lunak antivirus. Virus dapat berasal dari lampiran dalam pesan email, file pada CD atau DVD, atau file yang diunduh dari Internet. Pastikan perangkat lunak antivirus mutakhir dan diatur untuk memindai komputer Anda secara teratur. Ada banyak program antivirus yang tersedia. Microsoft menawarkan Security Essentials, program antivirus gratis yang dapat Anda unduh dari situs web Microsoft Security Essentials.

Anda juga dapat mengunjungi situs web penyedia perangkat lunak Keamanan Windows untuk menemukan program antivirus pihak ketiga.

Menggunakan router untuk berbagi koneksi Internet: Pertimbangkan untuk menggunakan router untuk berbagi koneksi Internet. Perangkat ini biasanya memiliki firewall bawaan, terjemahan alamat jaringan (NAT), dan fitur lain yang dapat membantu menjaga jaringan Anda lebih terlindungi dari peretas.

Jangan tetap masuk sebagai administrator: Saat Anda menggunakan program yang memerlukan akses Internet, seperti browser web atau program email, kami menyarankan Anda masuk sebagai akun pengguna standar daripada akun administrator. Itu karena banyak virus dan worm tidak dapat disimpan dan dijalankan di komputer Anda kecuali Anda masuk sebagai administrator.

Rekomendasi keamanan jaringan nirkabel: Jika Anda memiliki jaringan nirkabel, ada beberapa tindakan pencegahan keamanan tambahan yang harus Anda ambil. Gunakan kunci keamanan jaringan: Jika Anda memiliki jaringan nirkabel, Anda harus mengatur kunci keamanan jaringan, yang mengaktifkan enkripsi. Dengan enkripsi, orang tidak dapat terhubung ke jaringan Anda tanpa kunci keamanan. Selain itu, setiap informasi yang dikirim melalui jaringan Anda dienkripsi sehingga hanya komputer yang memiliki kunci untuk mendekripsi informasi yang dapat membacanya. Ini dapat membantu mencegah upaya untuk mengakses jaringan dan file Anda tanpa izin Anda. Wi-Fi Protected Access (WPA atau WPA2) adalah metode enkripsi jaringan nirkabel yang direkomendasikan.

Mengubah nama dan kata sandi administrator default pada perute atau titik akses Anda: Jika Anda memiliki perute atau titik akses, Anda mungkin menggunakan nama dan kata sandi default untuk menyiapkan peralatan. Sebagian besar produsen menggunakan nama dan kata sandi default yang sama untuk semua peralatan mereka, yang dapat digunakan seseorang untuk mengakses router atau titik akses Anda tanpa sepengetahuan Anda. Untuk menghindari risiko itu, ubah nama pengguna dan kata sandi administrator default untuk router Anda. Periksa informasi yang disertakan dengan perangkat Anda untuk petunjuk tentang cara mengubah nama dan sandi.

Mengubah SSID default: Router dan titik akses menggunakan nama jaringan nirkabel yang dikenal sebagai service set identifier (SSID). Sebagian besar produsen menggunakan SSID yang sama untuk semua router dan titik akses mereka. Kami menyarankan Anda mengubah SSID default agar jaringan nirkabel Anda tidak tumpang tindih dengan jaringan nirkabel lain yang mungkin menggunakan SSID default. Ini memudahkan Anda untuk mengidentifikasi jaringan nirkabel mana yang menjadi milik Anda, jika ada lebih dari satu di sekitar, karena SSID biasanya ditampilkan dalam daftar jaringan yang tersedia. Periksa informasi yang disertakan dengan perangkat Anda untuk petunjuk tentang cara mengubah SSID default.

Posisikan router atau titik akses Anda dengan hati-hati: Sinyal nirkabel dapat mengirimkan beberapa ratus kaki, sehingga sinyal dari jaringan Anda dapat disiarkan di luar rumah Anda. Anda dapat membantu membatasi area jangkauan sinyal nirkabel Anda dengan memposisikan router atau titik akses Anda di dekat pusat rumah Anda daripada di dekat dinding atau jendela luar.

1.7 WINDOWS-MICROSOFT: BANTUAN UNTUK MELINDUNGI PC5 ANDA

Akun untuk setiap pengguna komputer

Saat pertama kali mengatur Windows, Anda harus membuat akun administrator. Akun administrator memberi Anda kendali penuh atas komputer, perangkat lunak apa yang harus diinstal, dan siapa lagi yang dapat menggunakannya. Anda dapat menggunakan akun administrator untuk menyiapkan akun pengguna standar untuk pengguna lain. Jika Anda berbagi komputer di rumah dengan orang lain, seperti anak, suami, atau istri Anda, akun pengguna standar yang terpisah untuk setiap pengguna memungkinkan setiap orang masuk ke pengalaman yang dipersonalisasi. Misalnya, Anda dapat mengatur latar belakang desktop Anda ke gambar dari liburan Hawaii Anda, sementara putra remaja Anda mungkin memiliki latar belakang bergulir hot rods yang disesuaikan. Atau sebaliknya. Akun pengguna juga menentukan izin yang dimiliki setiap pengguna untuk mengakses file dan program yang berbeda atau mengubah pengaturan komputer. Setiap orang yang secara teratur menggunakan komputer Anda harus memiliki akun standar, sehingga mereka dapat menyesuaikan pengalaman mereka tanpa memengaruhi pengguna lain. Untuk informasi lebih lanjut, lihat Akun pengguna: pertanyaan umum.

Kata yang kuat tentang kata sandi

Kata sandi adalah salah satu cara termudah untuk membantu melindungi komputer Anda dari peretas, anak-anak Anda, atau pengguna yang tidak berwenang. Sama seperti PIN kartu debit Anda adalah penghalang antara orang jahat dan rekening bank Anda, kata sandi komputer adalah penghalang antara pengguna yang tidak sah dan akun pengguna Anda. Untuk detail selengkapnya, lihat Melindungi komputer Anda dengan kata sandi.

Saat Anda memilih kata sandi, Anda harus mempersulit orang lain untuk menebak atau memecahkannya. Ayah saya mempelajari ini dengan cara yang sulit ketika dia mengatur kata sandinya menjadi huruf "A." Adikku dan aku menguraikannya dengan tergesa-gesa dan mengkonfigurasi ulang desktopnya untuk kegembiraan maksimum (kami) dan gangguan maksimum (Ayah). Kata sandi yang kuat tidak boleh terlalu jelas—jadi nama Anda, nama hewan peliharaan Anda, atau tanggal lahir Anda bukanlah kandidat kata sandi terbaik. Untuk mempelajari lebih lanjut, lihat Kiat untuk membuat kata sandi dan frasa sandi yang kuat.

Kontrol Akun Pengguna: Ibu, bolehkah?

Fitur Kontrol Akun Pengguna (UAC) di Windows adalah cara lain untuk membantu Anda mengontrol perubahan signifikan pada komputer Anda. Jika Anda ingin membuat perubahan yang memerlukan izin administrator—seperti menginstal perangkat lunak baru atau mengubah pengaturan Windows—UAC akan memberi tahu Anda. Jika Anda menggunakan akun administrator, Anda akan diminta untuk mengonfirmasi perubahan. Pengguna standar diminta untuk memasukkan kata sandi administrator sebelum perubahan dapat dilakukan.

Bantu lindungi PC Anda dari ancaman online

Kiat di atas dapat membantu melindungi komputer Anda dari kecelakaan keamanan di rumah, tetapi saat Anda menggunakan Internet, Anda perlu mempertimbangkan tindakan pencegahan lainnya. Anda harus membuat rencana keamanan yang baik, menjaganya tetap terkini, dan menggunakan sedikit akal sehat sehari-hari.

Gunakan perangkat lunak keamanan

Pikirkan Windows Firewall sebagai penghalang antara komputer Anda dan peretas perampok (atau spammer yang tidak diminta) di Internet. Windows Firewall memeriksa informasi yang masuk dan keluar dari komputer Anda. Jika informasi tersebut tampak aman, informasi tersebut akan diteruskan. Jika informasi tersebut tampaknya berasal dari sumber yang tidak jelas atau berisi perangkat lunak berbahaya (seperti worm atau virus), firewall dapat membantu memblokirnya dan juga membantu mencegah komputer Anda menyebarkan perangkat lunak berbahaya ke orang lain jika sudah terinfeksi. Windows Firewall diaktifkan secara default, tetapi Anda dapat memilih untuk mengizinkan program tertentu—seperti pesan instan—melalui firewall, atau Anda dapat memblokir semua koneksi masuk ke komputer Anda jika Anda menggunakan jaringan publik di bandara atau kedai kopi. Untuk informasi selengkapnya, lihat Memahami pengaturan Windows Firewall.

Spyware mungkin mengganggu Anda dengan menampilkan iklan pop-up atau menambahkan bilah alat dan tautan yang tidak diinginkan di browser web Anda—atau mungkin secara diam-diam mengumpulkan informasi tentang Anda dan penggunaan komputer Anda dan mengirimkan informasi itu kembali ke orang lain. Untuk membantu melindungi komputer Anda dari spyware, Anda dapat menggunakan program antispyware seperti Windows Defender. Windows Defender juga diaktifkan secara default, dan dapat memindai komputer Anda dari spyware yang ada untuk menghapusnya atau memperingatkan Anda ketika spyware baru mencoba menginstal sendiri. Untuk informasi selengkapnya, lihat Menggunakan Windows Defender.

Anda juga harus menginstal perangkat lunak antivirus untuk memindai email dan file lain dari program yang merusak dan memblokirnya. Virus, worm, dan Trojan horse tidak selalu mengekspos informasi pribadi Anda kepada orang lain, tetapi mereka dapat menghapus file penting dan memperlambat atau bahkan menonaktifkan komputer Anda sepenuhnya. Sebagian besar virus juga dapat mereplikasi dan mendistribusikan dirinya sendiri melalui email ke semua kontak Anda, cara cepat untuk membuat musuh keluar dari teman di buku alamat Anda. Untuk membantu mencegah hal ini terjadi. Anda dapat mengunduh Microsoft Security Essentials, program antivirus gratis dari Microsoft, dengan mengunjungi situs web Microsoft Security Essentials. Anda juga dapat mengunjungi halaman web penyedia perangkat lunak keamanan konsumen Windows 7 untuk menemukan program antivirus pihak ketiga.

Pantau dan perbarui rencana keamanan Anda: Orang jahat rajin, jadi perangkat lunak keamanan Anda hanya sebaik yang terbaru. Tetapi melacak pembaruan keamanan, dan membuatnya secara otomatis, lebih mudah di Windows 7 dengan Pusat Aksi baru.

1.8 MANAJEMEN KEAMANAN DATA

Manajemen keamanan data adalah cara untuk menjaga integritas data dan memastikan bahwa data tidak dapat diakses oleh pihak yang tidak berwenang atau rentan terhadap korupsi data. Keamanan data diberlakukan untuk memastikan privasi selain atau melindungi data ini. Data itu sendiri adalah bentuk mentah dari informasi yang disimpan di server jaringan, kemungkinan komputer pribadi dan dalam bentuk kolom dan baris. Data ini dapat berupa apa saja mulai dari file pribadi hingga kekayaan intelektual dan bahkan informasi rahasia. Data dapat dianggap sebagai segala sesuatu yang dapat dipahami dan diinterpretasikan oleh manusia.

Karena internet adalah fenomena yang berkembang, ada dan akan selalu menekankan pada perlindungan data pribadi atau perusahaan. Pengguna komputer seiring berjalannya waktu cenderung sedikit lebih sadar dengan file mereka, tetapi masih didorong untuk menggunakan semacam keamanan data. Metode keamanan data dapat diperoleh dengan menggunakan solusi perangkat lunak atau mekanisme perangkat keras tertentu.

Informasi dapat dienkripsi atau tidak dapat dibaca oleh orang yang tidak memiliki akses. Saat mengenkripsi data ini, urutan matematika dan algoritma digunakan untuk mengacak informasi. Enkripsi hanya mengizinkan pihak yang disetujui untuk memecahkan kode teks yang tidak dapat dibaca ini dengan kunci. Hanya mereka yang memiliki kunci ini yang dapat mengakses informasi apa pun. Otentikasi adalah bentuk lain dari keamanan data yang akan digunakan untuk akses harian. Masuk ke akun email, rekening bank, dll., Hanya mengizinkan pengguna dengan kunci atau kata sandi yang tepat. Metode yang paling umum digunakan untuk menjaga data tetap terlindungi adalah dengan perangkat lunak keamanan data. Perangkat lunak ini mencegah pihak yang tidak berwenang mengakses data pribadi dan menawarkan berbagai opsi berbeda. Beberapa opsi ini termasuk mengharuskan masuk ke akun email, menulis ulang perangkat lunak, dan dapat mengontrol opsi keamanan dari jarak jauh. Data juga dapat dilindungi dengan keamanan IP. Artinya, data dapat dilindungi dari peretas saat dalam perjalanan.

Salah satu alasan terbesar untuk menjaga data tetap terlindungi adalah karena ada banyak perusahaan yang ingin ditargetkan dan dilanggar oleh peretas. Keamanan data cenderung diperlukan untuk bisnis besar tetapi yang kecil biasanya memiliki infrastruktur yang lebih sedikit, membuat informasi tidak menjadi kerugian besar jika dilanggar. Tergantung pada layanan dan konten yang akan dilindungi, mungkin ada tindakan pencegahan untuk melindungi informasi lebih lanjut. Misalnya Windows Rights Management Services (RMS) dapat diatur untuk mengontrol apakah penerima email dapat dibaca dan dilihat, diedit, disalin atau disimpan; pengaturan ini juga dapat mengatur tanggal kedaluwarsa dokumen tertentu.

Dengan menjaga keamanan data, dimungkinkan untuk memberikan akses yang berbeda ke orang yang berbeda. Misalnya, rekanan penjualan dapat memiliki akses ke basis data penjualan mereka, tetapi tidak dapat mengakses informasi rekanan penjualan atau informasi bisnis lainnya (misalnya hutang dagang, piutang dagang). Membuat satu lokasi penyimpanan (atau server) untuk data, dan menugaskan individu dengan akses berbeda, mengikuti data sangat mudah. Itu membuatnya lebih mudah untuk memelihara data, dan memungkinkan transfer cepat ke lokasi penyimpanan lain jika diperlukan. Perangkat lunak keamanan data juga dapat berfungsi sebagai sumber untuk membuat situs yang aman (yang memberikan akses ke file data) hanya dapat diakses oleh personel yang berwenang.

1.9 MANAJEMEN KUALITAS DATA PERUSAHAAN

Bagian ini menjelaskan Kerangka Manajemen Kualitas Data Perusahaan (CDQM). Ini mendukung organisasi dalam penilaian dan analisis solusi untuk peluang yang terlewatkan dan potensi CDQM yang belum dimanfaatkan. Ini didasarkan pada Model Keunggulan EFQM - yang digunakan oleh lebih dari 30.000 organisasi di dunia - dan memberi organisasi kesempatan untuk mengoordinasikan kegiatan CDQM dengan menerapkan pendekatan nilai yang ditunjukkan. Selanjutnya, Framework dapat digunakan dalam beberapa cara:

- sebagai alat untuk membandingkan dengan organisasi lain,
- sebagai panduan untuk mengidentifikasi area untuk perbaikan dan meningkatkan kesadaran akan kualitas data perusahaan,
- sebagai kosakata umum dan cara berpikir,
- dan sebagai kerangka kerja di mana kemampuan CDQM dapat dikembangkan.

Kerangka untuk CDQM membahas para profesional dalam organisasi yang berhubungan dengan pengelolaan dan individu-individu yang mendapatkan manfaat dari kualitas data perusahaan yang baik. Perspektif Bisnis tentang Kualitas Data Perusahaan Organisasi perlu menanggapi sejumlah penggerak bisnis di mana data perusahaan berkualitas tinggi merupakan prasyarat penting.

- Manajemen risiko dan kepatuhan
- Manajemen pelanggan terintegrasi
- Integrasi, otomatisasi, dan standarisasi proses bisnis
- Pelaporan
- Konsolidasi TI

Isi:

- Tujuan dokumen
- Perspektif bisnis terhadap Kualitas Data Perusahaan
- Konsep dasar

Manajemen Kualitas Data Perusahaan

Data Perusahaan dan Kualitas Data Induk Aspek Manajemen Data Perusahaan Kualitas Data Perusahaan

- Model Keunggulan EFQM
- RADAR

Model Keunggulan EFQM dan Kerangka Kerja untuk Manajemen Kualitas Data Perusahaan

- Kerangka Kerja Manajemen Kualitas Data Perusahaan
- Pemberdaya
    - Strategi
    - Pengendalian
    - Organisasi & Orang
    - Proses & Metode
    - Arsitektur Data
    - Aplikasi
    - Hasil
    - Hasil Pelanggan
    - Hasil Orang
    - Hasil Masyarakat
    - Hasil Bisnis

Menerapkan Kerangka Kerja Kualitas Data Perusahaan Pengelolaan

- Proses Penilaian Diri
- Memilih teknik Penilaian Diri yang tepat
    - Bantuan lebih lanjut

- Sumber daya EFQM
- Sumber daya CDQM
- Konsorsium CC CDQ
- Alat

1.10 KEAMANAN DAN PRIVASI- DATA ADALAH KUNCINYA

Dengan meningkatnya visibilitas pelanggaran keamanan data, organisasi dan regulator sama-sama menekankan perlindungan informasi sensitif. Saat ini, memastikan perawatan data yang tepat telah menjadi fokus utama keamanan informasi dan manajemen privasi. Namun, tantangannya lebih kompleks daripada yang disadari banyak orang. Banyak yang mungkin berasumsi bahwa menerapkan teknik seperti enkripsi ke data saat istirahat atau dalam perjalanan adalah dasar untuk mengamankan informasi sensitif.

Faktanya, fondasi yang lebih realistis tergantung pada penanganan masalah paparan data. Informasi digital dapat dengan mudah diduplikasi, dan sering dibagikan secara luas. Organisasi mungkin atau mungkin tidak menyadari apa – atau di mana – aset informasi mereka yang paling sensitif, bagaimana mereka digunakan, dan apa yang terjadi pada informasi ini sepanjang siklus hidupnya. Mereka dapat membuat salinan data yang berlebihan tanpa perlu, meningkatkan eksposur hanya untuk memfasilitasi tujuan seperti pengembangan aplikasi atau pelatihan. Ketika tindakan perlindungan diperlukan, teknik modern memberikan pilihan yang lebih fleksibel, termasuk yang mengatasi salah satu kesenjangan paparan yang paling signifikan dari semuanya: perlindungan informasi saat digunakan. Salah satu teknik tersebut adalah data masking. Saat sumber data diakses, penyembunyian mengaburkan elemen yang lebih sensitif seperti informasi yang dapat diidentifikasi secara pribadi saat mengirimkan data yang berguna. Hal ini dilakukan, bukan dengan menimpa data dalam database produksi, tetapi dengan mengganti nilai sensitif dengan pengganti yang realistis (tetapi tidak aktual) saat data dikirimkan ke pengguna atau aplikasi yang mengonsumsi.

- Saat pengembang membangun aplikasi yang berpusat pada data, mereka harus memastikan fungsionalitas yang lengkap dan menyelesaikan masalah operasional apa pun. Ini mungkin sulit jika bukan tidak mungkin kecuali aplikasi dapat berinteraksi dengan data aktual atau lingkungan produksi. Memfilter elemen data sensitif secara manual mungkin tidak praktis. Ini dapat mengganggu dependensi aplikasi penting seperti format data, atau meninggalkan celah yang mengekspos item sensitif. Pengujian integrasi tahap akhir tanpa akses ke database produksi dapat menghasilkan hasil yang tidak lengkap dan menyesatkan. Pengembangan dan pengujian dengan demikian telah menjadi salah satu aplikasi penyembunyian data yang lebih terlihat.
- Teknik ini memungkinkan penggunaan informasi aktual yang lebih transparan – seperti kumpulan data populasi yang digunakan untuk menganalisis tren kesehatan atau kecelakaan, misalnya – tanpa memaparkan informasi pribadi masing-masing subjek. Algoritma masking sering dirancang agar dapat diulang, sehingga integritas referensial dari data masking dipertahankan.
- Baru-baru ini, penggunaan teknik penyamaran secara real time (sebagai lawan penyamaran salinan statis dari kumpulan data) telah meningkatkan nilai maskiha. Teknik penyembunyian "dinamis" semacam itu memungkinkan interaksi yang lebih

langsung dengan data produksi – dan tidak hanya untuk pengembangan dan pengujian. Kemampuan untuk mengirimkan data secara selektif, atau bagian dari kumpulan data, dapat secara signifikan meningkatkan jangkauan dan fleksibilitas aplikasi yang mengandalkan penyimpanan data sensitif. Penyembunyian dinamis sebaris dapat mencapai ini tanpa memerlukan modifikasi basis data target atau aplikasi yang mengandalkan. Ini juga mengurangi eksposur risiko dengan menghilangkan kebutuhan untuk membuat salinan sumber data. Bersama-sama, kemampuan ini mengurangi risiko serta biaya.

Namun, untuk mewujudkan manfaat maksimal, penyembunyian data – serta teknik perlindungan lainnya – dapat dimanfaatkan dengan baik jika diintegrasikan dengan pendekatan strategis terhadap manajemen informasi.
Penuh arti:

- Bagaimana dan kapan data dibuat dan dimodifikasi;
- Bagaimana data digunakan dan diintegrasikan dengan aplikasi atau sumber data lainnya;
- Proses yang diperlukan untuk menjamin integritas data; dan
- Bagaimana data akhirnya disimpan atau dihentikan

Memungkinkan organisasi untuk memahami bagaimana dan di mana teknik seperti masking dapat diterapkan paling efektif. Kombinasi penemuan dan penyembunyian data dengan otomatisasi sub-pengaturan data, misalnya, dapat mengoptimalkan teknik perlindungan data bersama dengan integrasi data dan teknologi manajemen siklus hidup informasi. Ini memastikan pengiriman hanya informasi yang diperlukan tanpa mengganggu dependensi data penting, ketika keamanan dan manajemen risiko terintegrasi dengan manajemen informasi perusahaan. Namun, relevansi informasi dengan upaya keamanan lebih dari sekadar melindungi informasi itu sendiri. Semakin banyak, organisasi mencari teknologi berbasis data saat ini untuk meningkatkan wawasan yang akurat dan tepat waktu tentang ancaman dan strategi dasar pada penilaian yang lebih objektif - dan berdiri di persimpangan penting dari kepentingan berbasis data tersebut adalah kemampuan integrasi data, rasionalisasi dan analisis yang membuat teknologi seperti Manajemen Acara Kompleks lebih berharga untuk upaya ini daripada sebelumnya.

1.11 RINGKASAN

Keamanan dan manajemen data adalah konsep yang sangat penting dari E-security. Dalam unit ini berbagai konsep penting dibahas panjang lebar untuk pemahaman dan penerapan yang lebih baik di tempat yang tepat. Terutama konsep keamanan data, melindungi data sensitif, data sensitif browser, tata kelola data, penjelajah internet dan keamanan jaringan, peran window-Microsoft: membantu melindungi OC Anda, manajemen keamanan data, manajemen kualitas data perusahaan dan keamanan & privasi data di kunci dibahas panjang lebar untuk memahami unit sepenuhnya.

1.12 BEBERAPA BUKU BERGUNA

1. Black Ice: Ancaman Terorisme Cyber yang Tak Terlihat oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
2. Cyber Crime dan Cyber Terrorism oleh R.K. Pradhan (Publikasi Mangalam)
3. Cyber Crime dan Cyber Terrorism oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
4. Terorisme Cyber oleh S. Venkatesh (Penulis)
5. Keamanan Crypto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
6. Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
7. Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
8. Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
9. Buku Pegangan Keamanan, Kriptografi dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
10. Hukum Cyber dan Perlindungan IT oleh Harsh Cander (Publikasi PHI)
11. Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
12. Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
13. Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
14. Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
15. Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
16. Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
17. Ruang Siber dan Keamanan Siber oleh Progressive Management (Publikasi Manajemen Progresif)
18. Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
19. Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

1.13 PERIKSA KEMAJUAN ANDA

A. Manakah dari pernyataan berikut ini yang benar atau salah:

1. Keamanan komputer adalah masalah yang tidak terpecahkan.
2. Keamanan data juga melindungi data dari korupsi.
3. Kembali di Musim Panas 2013 Google dikritik karena menyimpan informasi login pengguna, nama pengguna dan kata sandi dalam teks biasa di browser web tanpa perlindungan apa pun.
4. Semua program tata kelola data tidak sama.
5. Manajemen keamanan data adalah cara untuk menjaga integritas data.

B. Isi Bagian yang Kosong:

1. Keamanan data disebut juga sebagai .....atau keamanan komputer.
2. Tata kelola data mengacu pada pengelolaan keseluruhan .....data.
3. ..... dapat membantu mencegah peretas atau perangkat lunak berbahaya (seperti worm).
4. ..... adalah salah satu cara yang lebih mudah untuk membantu melindungi komputer Anda dari peretas.
5. ..... dapat dengan mudah diduplikasi, dan sering dibagikan secara luas.

1.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Keamanan Informasi
2. Ketersediaan, kegunaan, integritas, dan keamanan
3. Firewall
4. Kata Sandi
5. Informasi Digital

1.15 PERTANYAAN TERMINAL

1) Apa itu keamanan data?
2) Tentukan perlindungan data sensitif.
3) Membahas secara detail tata kelola data dan CDQM.
4) Apakah data keamanan dan privasi adalah kunci untuk melindungi komputer dari peretas?
5) Apa itu penjelajah internet dan keamanan jaringan?

BAB 2
TATA KELOLA ELEKTRONIK

Tujuan:
Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan E-Governance
- Memahami pentingnya E-Governance dalam Tata Kelola dan Pembangunan yang Baik
- Memahami masalah teknis dan hukum terkait E-Governance

2.1 PENGANTAR

Munculnya e-government telah menjadi salah satu perkembangan web yang paling mencolok. Ketika komunitas digital yang didukung Internet berkembang, dan dengan asumsi bahwa mereka memang tumbuh untuk menggabungkan individu di seluruh negeri (dan dunia), mereka menghadirkan sejumlah tantangan dan peluang kepada pemerintah nasional. Pemerintah di negara-negara demokratis terutama merupakan mekanisme perwakilan di mana beberapa orang terpilih memperdebatkan dan memberlakukan undang-undang untuk dan atas nama warga negara negara bangsa. Ada beberapa aspek yang mungkin terbukti penting dalam konteks e-governance. Pertama, wakil-wakil terpilih itu membutuhkan akses ke sumber informasi dan komunikasi. Penting bagi mereka untuk menginformasikan dan mendengarkan konstituen mereka; perlu bagi mereka untuk berkomunikasi satu sama lain; dan paling-paling, perlu bagi mereka untuk menemukan dan mewakili keinginan mereka yang telah memilih mereka sebagai wakil mereka. Sementara kami memilih individu, kami menghargai dan memahami bahwa mereka kemudian harus menyeimbangkan tiga kekuatan yang terkadang berlawanan: hati nurani mereka sendiri; filosofi partai mereka; dan kepentingan konstituen mereka sendiri. Pada tingkat yang paling sederhana, implementasi e-governance kemudian dapat mendukung kebutuhan informasi dan komunikasi ini. E-mail antara politisi dan antara politisi dan departemen dapat dengan mudah dibuat. Karena banyak pemerintah negara bagian.

Menyediakan Lap top untuk anggota parlemen dan MLA mereka, mereka dapat mempublikasikan halaman rumah mereka di Internet, untuk bertindak sebagai pusat interaksi konstituen. Ini kemudian menyentuh aspek berikutnya, yaitu berkomunikasi dengan konstituen. Selain saluran dan mekanisme standar, politisi dapat menerima pesan email dari mereka yang ingin mengekspresikan pandangan mereka. Ada cara serupa yang tak ada habisnya untuk memanfaatkan teknologi Informasi dan komunikasi (hanya dibatasi oleh imajinasi lembaga pelaksana) untuk memberikan solusi yang efisien dan transparan kepada warga.

2.2 SEJARAH E-GOVERNANCE DI INDIA

Di antara negara-negara berkembang, India telah menjadi pengadopsi awal e-governance. Gelombang pertama dapat dianggap telah berevolusi dari bawah ke atas. Beberapa wirausaha sosial meyakinkan pejabat tingkat kabupaten tentang keajaiban TIK baru, terutama dalam menyediakan layanan konvergen ke daerah terpencil, dan meningkatkan

transparansi dan pengawasan dalam hal ini. Proyek Gyandoot di distrik Dhar, yang dimulai pada tahun 2000, dianggap sebagai cikal bakal dari apa yang akan menjadi serangkaian proyek yang membangun front-end di banyak komunitas desa yang seharusnya dilayani oleh back-end sebagian besar di distrik tersebut. mengumpulkan orat. Ide dan upayanya adalah untuk menciptakan tekanan dari front-end komunitas untuk digitalisasi proses departemen back-end. Yang terakhir ini sebagian besar merupakan upaya lokal, sebagian besar bergantung pada inisiatif dan energi dari kolektor distrik yang bersangkutan, seringkali dengan beberapa dukungan yang sangat bersemangat dari staf National Informatics Center (NIC) distrik. Mungkin upaya yang paling terorganisir dan berhasil dalam fase pertama e-governance di India, kira-kira antara tahun 2000-05, adalah e-Seva Pedesaan di distrik Godavari Barat di Andhra Pradesh. Adapun untuk pengembangan ujung depan tingkat komunitas dua inisiatif, N-log dan Drishti menonjol, yang masing-masing pada satu waktu diklaim menjalankan ribuan telecaster komunitas di seluruh negeri yang dapat memberikan layanan e-governance.

Ada kecenderungan umum untuk mengklasifikasikan upaya awal ini sebagai kegagalan. Memang, sekitar 2005-06, N-logue ditutup dan Drishti pindah dari layanan e-governance. E-Seva pedesaan juga tidak pernah ditingkatkan. Namun, yang perlu diperhatikan adalah bahwa dalam waktu yang relatif singkat, proyek-proyek awal ini menciptakan kesan abadi tentang TIK baru sebagai sarana yang memungkinkan untuk mendekatkan pemerintahan kepada masyarakat, dan mungkin juga membuatnya lebih transparan dan akuntabel. Sejauh itu, mereka memiliki dampak yang sangat signifikan, bahkan jika inisiatif ini sendiri tidak dapat bertahan, karena berbagai alasan yang tidak dapat kita bahas secara lebih rinci, di sini. (Namun, jika kita membandingkan situasi ini dengan ledakan gelembung dotcom di awal dekade terakhir, kita dapat melihat beberapa faktor umum.) Mereka menciptakan konteks untuk Rencana E-Governance Nasional (NEGP) yang sangat ambisius, terutama proyek andalannya, Pusat Layanan Umum, yang diresmikan oleh Pemerintah India pada tahun 2006.

Sementara itu, banyak proyek digitalisasi dan otomatisasi tingkat departemen independen mulai terbentuk. Digitalisasi catatan kepemilikan dan transaksi tanah telah menjadi salah satu bidang utama dengan dampak yang cukup besar, karena merupakan daerah yang sangat penting dan menjengkelkan bagi pedesaan India. Dalam banyak kasus, digitalisasi ujung ke ujung difasilitasi oleh perubahan signifikan dalam peraturan pemerintah, yang memberikan beberapa contoh awal rekayasa ulang proses e-governance skala penuh. Beberapa kegiatan otomasi lainnya seperti komputerisasi perbendaharaan pemerintah dan transaksi keuangan juga memiliki dampak yang cukup besar pada efisiensi fungsi pemerintahan, dan sebagian besar mewakili upaya e-governance yang berhasil dan berkelanjutan.

Sejak awal, upaya juga dilakukan untuk mengkomputerisasi alur kerja di kantor-kantor pemerintah, seperti inisiatif e-Sekretariat di beberapa negara bagian. Namun, prakarsa-prakarsa tersebut gagal untuk dipertahankan karena tampaknya bertentangan dengan cara-cara formal dan informal fungsi birokrasi India. Setiap kemajuan di bidang dasar seperti kegiatan pemerintah yang membutuhkan perubahan perilaku yang signifikan, dan juga memiliki implikasi yang sangat signifikan untuk transparansi dan akuntabilitas yang lebih besar, akan membutuhkan dorongan legislatif yang kuat.

2.3 ASAL E-GOVERNANCE DI INDIA (PUSAT INFORMATIKA NASIONAL)

Pusat Informatika Nasional (NIC) didirikan pada tahun 1976, dan sejak itu muncul sebagai "pembangun utama" aplikasi e-Government / e-Governance hingga tingkat akar rumput serta promotor peluang digital untuk pembangunan berkelanjutan. NIC, melalui Jaringan ICT-nya, "NICNET", memiliki hubungan kelembagaan dengan semua Kementerian/Departemen Pemerintah Pusat, 35 Pemerintah Negara Bagian/Wilayah Serikat, dan sekitar 625 administrasi Distrik di India. NIC telah berperan penting dalam mengarahkan aplikasi e-Government/e-Governance di kementerian/departemen pemerintah di Pusat, Negara Bagian, Distrik dan Blok, memfasilitasi peningkatan layanan pemerintah, transparansi yang lebih luas, mempromosikan perencanaan dan manajemen yang terdesentralisasi, menghasilkan efisiensi dan akuntabilitas yang lebih baik kepada rakyat India.

Program "Informatics-led-development" dari pemerintah telah dipelopori oleh NIC untuk memperoleh keunggulan kompetitif dengan menerapkan aplikasi TIK dalam administrasi sosial & publik. Kegiatan utama berikut sedang dilakukan:

- Menyiapkan Infrastruktur TIK
- Implementasi Proyek e-Governance Tingkat Nasional dan Negara Bagian
- Produk dan layanan
- Konsultasi dengan departemen pemerintah
- Penelitian dan Pengembangan
- Peningkatan Kapasitas

Selama tiga dekade terakhir, NIC telah mengimplementasikan banyak perangkat lunak aplikasi "pusat jaringan" untuk implementasi Program di berbagai kementerian dan departemen, menggunakan perangkat lunak canggih. Selama 1980-an dan awal 1990-an, dorongan kebijakan adalah menciptakan "Sistem Informasi Manajemen (SIM)" dan "Sistem Pendukung Keputusan (DSS)" untuk pembangunan, perencanaan dan administrasi responsif di pemerintahan yang mengarah pada asal-usul hari ini "e -Governance" / "e- Government".

Konsep "Menjembatani Kesenjangan Digital", "Inklusi Sosial dan Keuangan melalui TIK" dan "Menjangkau Yang Belum Terjangkau" dicoba dan dioperasikan pada akhir tahun sembilan puluhan. NIC memiliki keahlian dan pengalaman yang luas dalam desain, pengembangan, dan operasionalisasi berbagai proyek e-Government di bidang Administrasi dan Tata Kelola Publik seperti Pertanian & Pangan, Peternakan, Perikanan, Kehutanan & Lingkungan, Industri, Kesehatan, Pendidikan, Anggaran, dan Perbendaharaan , Sumber Daya Fiskal, Transportasi, Sumber Daya Air, Manajemen Pengadilan, Pembangunan Pedesaan, Catatan Tanah dan Pendaftaran Properti, Kebudayaan & Pariwisata, Fasilitasi Impor & Ekspor, Layanan Kesejahteraan Sosial, Perencanaan Tingkat Mikro, dll. Dengan meningkatnya kesadaran yang mengarah pada permintaan dan ketersediaan Infrastruktur TIK dengan kapasitas dan kerangka program yang lebih baik, ruang tata kelola di negara ini menyaksikan babak baru proyek dan produk, yang mencakup seluruh spektrum e-Governance termasuk G2C, G2B, G2G, dengan penekanan pada pemberian layanan.

NIC menyediakan Infrastruktur ICT Umum Nasional untuk mendukung layanan e-Governance kepada warga, Produk dan Solusi yang dirancang untuk mengatasi Prakarsa e-Governance, Proyek e-Governance Utama, Dukungan Informatika Negara Bagian/UT dan layanan tingkat distrik yang diberikan.

NIC telah menyiapkan infrastruktur TIK mutakhir yang terdiri dari Pusat Data Nasional dan negara bagian untuk mengelola sistem informasi dan situs web Kementerian/Departemen Pusat, Pusat Pemulihan Bencana, fasilitas Operasi Jaringan untuk mengelola jaringan heterogen yang tersebar di Bhawan, Negara Bagian dan Distrik, Otoritas Sertifikasi, Konferensi Video, dan pengembangan kapasitas di seluruh negeri. Jaringan Pengetahuan Nasional (NKN) telah dibentuk untuk menghubungkan lembaga/organisasi yang melakukan penelitian dan pengembangan, Pendidikan Tinggi dan Pemerintahan dengan kecepatan orde multi Gigabit per detik. Selanjutnya, sekretariat Pemerintah Negara Bagian terhubung ke Pemerintah Pusat melalui tautan berkecepatan sangat tinggi pada Kabel Serat Optik (OFC). Distrik-distrik terhubung ke masing-masing ibu kota negara bagian melalui leased line.

Berbagai inisiatif seperti Sistem Pengadaan Pemerintah (Geoponic), Perangkat Lunak Manajemen Perkantoran (Perkantoran), Sistem Manajemen Rumah Sakit (rumah sakit), Sistem Informasi Akuntansi Keuangan Pemerintah (Lekha), dll telah diambil yang dapat direplikasi di berbagai organisasi Pemerintah.

Karena NIC mendukung sebagian besar proyek e-Governance mode misi, bab tentang Proyek e-Governance Nasional mencantumkan rincian proyek ini yaitu Program Modernisasi Catatan Tanah Nasional (NLRMP), Transportasi dan Pendaftaran Nasional, Komputerisasi Perbendaharaan, PPN, MG-NREGA, India- Portal, e-Courts, Postal Life Insurance, dll. NIC juga meletakkan kerangka kerja dan merancang sistem untuk pemantauan online hampir semua skema pemerintah pusat seperti Integrated Watershed Management (IWMP), IAY, SGSY, NSAP, BRGF, Jadwal Suku dan Undang-Undang Penghuni Hutan Tradisional lainnya dll.

Dukungan TIK juga disediakan di Amerika Serikat/UT oleh NIC. Layanan yang berpusat pada warga juga diberikan secara elektronik di tingkat distrik, seperti Sertifikat Pendapatan, Sertifikat Kasta, dan Sertifikat Tempat Tinggal, dll., bersama dengan layanan lain seperti portal Beasiswa, izin, izin masuk, lisensi untuk beberapa nama. Dalam melaksanakan semua kegiatan tersebut, NIC telah diberikan pengakuan dalam hal penghargaan dan penghargaan di tingkat Internasional maupun Nasional, yang tercantum di Bagian Penghargaan.

Dengan demikian, NIC, sebuah program kecil yang dimulai oleh stimulus eksternal dari proyek UNDP, pada awal 1970-an, menjadi berfungsi penuh pada 1977 dan sejak itu telah berkembang dengan momentum yang luar biasa untuk menjadi salah satu S&T utama India; organisasi mempromosikan informatika memimpin pembangunan. Hal ini telah membantu mengantarkan transformasi yang diperlukan dalam pemerintahan agar mampu menghadapi tantangan milenium baru.

2.4 RENCANA E-GOVERNANCE NASIONAL

Fase kedua e-governance di India dapat dikatakan telah dimulai dengan peresmian National E-Governance Plan (NeGP) pada tahun 2006. Proyek unggulan NeGP berusaha untuk mendirikan sekitar 100.000 Common Service Center (CSC) di seluruh India, salah satunya untuk setiap enam desa. Baru-baru ini, Departemen TI menyatakan bahwa mereka telah mencapai target tersebut. NEGP juga terdiri dari 27 proyek Mode Misi, sebagian besar untuk komputerisasi back-end dari berbagai bidang kegiatan tata kelola. Selain itu, ia berupaya menciptakan infrastruktur e-governance nasional dari Jaringan Area Luas Negara Bagian, Pusat Data Negara, dan Gerbang Pengiriman Layanan Nasional.

Proyek dukungan infrastruktur dan teknis sebagian besar telah berjalan dengan baik. NEGP telah mampu memberikan pemahaman yang sama tentang urgensi, mekanisme, dan beberapa dukungan pendanaan untuk adopsi e-governance skala besar oleh berbagai departemen di pemerintah pusat dan negara bagian. Tindakan katalis seperti itu, dan mungkin menciptakan lingkungan untuk kinerja kompetitif, sangat dibutuhkan pada fase awal. Ini sangat berguna untuk negara-negara yang sebaliknya lambat dalam mengambil, yaitu e-governance, dan mereka mungkin juga yang paling membutuhkan reformasi tata kelola. Departemen TI memberikan dukungan teknis untuk inisiatif e-governance dari berbagai departemen di tingkat pusat dan negara bagian, termasuk melalui konsultan yang terdaftar. Mereka juga memastikan beberapa tingkat arsitektur umum yang sangat penting untuk interoperabilitas, terutama yang diperlukan ketika, pada tahap selanjutnya, integrasi operasi dan layanan lintas pemerintah dapat dicari.

Namun ada yang mencatat bahwa proyek yang berfokus pada penargetan bagian yang lebih kaya, mis. yang terkait dengan paspor dan pajak penghasilan, telah memberikan hasil terbaik hingga saat ini. Di sisi lain, Proyek Mode Misi di bidang-bidang seperti pertanian dan komputerisasi panchayat, yang paling langsung berkaitan dengan bagian-bagian yang relatif terpinggirkan, adalah yang paling lambat diluncurkan. Hal ini mungkin memerlukan penilaian ulang NEGP sehubungan dengan pertimbangan inklusi, kesetaraan dan keadilan sosial.

Meskipun ada beberapa kendala, proyek Unique ID, yang terdaftar sebagai Proyek Mode Misi di bawah NEGP, juga berjalan dengan baik. Baru-baru ini, Departemen TI telah membuat 'Framework for Mobile Governance' yang menjabarkan visi dan strategi untuk mobile governance. Ini membayangkan pengaturan Gateway Pengiriman Layanan Seluler, Toko Aplikasi Seluler untuk aplikasi tata kelola, otentikasi seluler dan gateway pembayaran, dan API3 untuk penyedia layanan yang berbeda. Departemen TI juga telah memberitahukan 'Kebijakan Standar Terbuka untuk E-governance', dan pekerjaan pemberitahuan standar terbuka di berbagai bidang sedang berlangsung. Tahun lalu, pedoman penggunaan media sosial oleh instansi pemerintah dikeluarkan oleh Departemen TI. Konsultasi internal dan pemangku kepentingan tentang peluang dan tantangan untuk e-governance di lingkungan komputasi awan juga sedang berlangsung. NEGP telah melakukan dengan sangat baik dalam memberikan dukungan infrastruktur dan teknis untuk adopsi e-governance secara luas di India. Namun, tampaknya ada kesenjangan yang signifikan di sisi non-teknis, yaitu arsitektur re-engineering proses tata kelola4 dan prinsip-prinsip sosial-politik yang luas yang perlu ditangani dan dalam e-governance. Sebagian besar karena NEGP, digitalisasi skala besar terjadi di sebagian besar departemen di pemerintah pusat dan negara bagian. Karena proses digitalisasi dan otomatisasi (tahap awal e-governance) telah berjalan dengan kecepatan yang stabil di seluruh lembaga pemerintah, proses ini telah menghasilkan peningkatan efisiensi yang substansial dan beberapa perbaikan di bidang transparansi. Jika keuntungan yang lebih besar di bidang transparansi, akuntabilitas dan partisipasi masyarakat belum tercapai, sebagian besar karena e-governance di India sebagian besar masih dipahami dan diimplementasikan dalam mode tekno-manajerial dan tanpa visi sosial-politik yang memadai.

Mungkin mengejutkan bagi banyak orang bahwa untuk area yang tidak hanya melibatkan dana hingga ribuan inti rupee dan juga sangat penting bagi masa depan pemerintahan di India, belum pernah ada kebijakan e-governance khusus di India. India.

Seseorang akan mengharapkan untuk memiliki semacam dokumen kebijakan yang terperinci berdasarkan konsultasi dengan semua pemangku kepentingan, yang memberikan visi untuk e-governance di India, mengintegrasikan prioritas reformasi tata kelola seperti desentralisasi, hak atas informasi, dan peningkatan partisipasi dan pemantauan masyarakat. Namun, pemeriksaan aktivitas dan tren e-governance di India membuktikan fakta bahwa e-governance di India tampaknya sebagian besar berjalan dengan logikanya sendiri, atau tidak ada logikanya. Pemahaman yang dominan tampaknya bahwa TI hanya membuat apa pun yang sedang dilakukan jauh lebih efisien, dan oleh karena itu mungkin tidak perlu masuk ke masalah dasar untuk memeriksa initio 'apa yang memang sedang dilakukan', 'apa yang seharusnya dilakukan' , dan 'bagaimana hal-hal sekarang dapat dilakukan dengan sangat berbeda'. Terserah mereka yang menjalankan sistem masing-masing untuk memutuskan apa yang mungkin ingin mereka lakukan dengan berbagai alat dan peluang TI. NEGP tampaknya hanya ada di sana untuk memberikan dukungan teknis; Sikap ini sering diutarakan oleh pejabat terkait.

Hal ini telah menyebabkan situasi di mana departemen sebagian besar menggunakan logika internal dan pertimbangan 'kepentingan' dan tujuan internal daripada terutama menggunakan logika eksternal, dari (1) sudut pandang tujuan dasar pemerintahan, dan peran khusus dari departemen mereka di dalamnya, (2) kebutuhan dan kemungkinan tanggapan pemerintah secara luas terhadap kebutuhan pemerintahan, dan, yang paling penting, (3) kebutuhan dan perspektif warga. Model matang e-governance di seluruh dunia berasal dari pertimbangan strategis tingkat yang lebih tinggi, sebelum mur dan baut perubahan tingkat departemen dan kantor yang sebenarnya dikerjakan.

Pendekatan tekno-manajerial seperti itu berarti bahwa e-governance di India tidak membuat hubungan yang jelas dengan bidang reformasi tata kelola lainnya seperti desentralisasi, hak atas informasi dan pemantauan masyarakat, sementara faktanya adalah bahwa proses rekayasa ulang melalui e-governance harus terutama telah melayani tujuan substantif reformasi pemerintahan di India. Anomali ini perlu dikoreksi melalui kebijakan e-governance nasional yang menempatkan e-governance dalam tujuan sosial-politik yang lebih besar dan kemudian dilanjutkan dengan menetapkan prinsip-prinsip tersebut yang harus memandu rekayasa ulang proses sistemik melalui e-governance. Prinsip-prinsip ini muncul dari kemungkinan tekno-sosial generik yang disediakan oleh masyarakat digital atau informasi. Prinsip-prinsip tersebut harus dapat menjelaskan dan mengakui perubahan teknologi yang cepat, dan membuka peluang baru lebih lanjut oleh TIK.

Desentralisasi, hak atas informasi dan pemantauan masyarakat, sebagai tiga bidang utama reformasi pemerintahan di India selain dari e-governance, semuanya bertujuan untuk partisipasi dan akuntabilitas dari bawah ke atas yang lebih besar. Mereka semua, bagaimanapun, membutuhkan, dan terus membutuhkan, legislasi pusat yang kuat dan dukungan kebijakan. Bahkan, mereka tidak dapat dicapai tanpa dorongan dan dukungan dari atas, dengan visi dan arah politik yang diartikulasikan dengan jelas. E-governance harus menjadi lebih dari sekedar menerapkan teknologi pada proses yang ada, dan harus dilihat dari potensi transformasinya. Untuk ini, ia juga harus diversi dan diartikulasikan dalam kaitannya dengan tujuan sosial-politik tertinggi dari reformasi pemerintahan di India. Tujuan ini kemudian harus diterjemahkan ke dalam prinsip tingkat yang lebih tinggi untuk arsitektur

proses e-governance, yang cukup umum dan fleksibel untuk diterapkan pada berbagai aktivitas dan sistem tata kelola.

Namun, memang benar bahwa e-governance di India didirikan di lingkungan di mana TIK baru menguasai dunia, dan tidak ada yang bisa dengan mudah menilai apa yang bisa dicapai dengan menggunakan TIK dalam pemerintahan, dan bagaimana caranya. Oleh karena itu diperlukan untuk melalui periode eksperimen yang intens. Ini merupakan penghargaan kepada para pemimpin awal e-governance di India bahwa mereka tidak menghindar dari keharusan berinvestasi ke dalam apa yang sebagian besar merupakan eksperimen intensif waktu dan sumber daya. Namun, mungkin sekarang saatnya untuk mengkonsolidasikan pembelajaran kita dan mulai mengambil pandangan yang lebih strategis dan sistemik dari reformasi tata kelola di India. Visi dan kebijakan yang jelas untuk tujuan ini mungkin merupakan prasyarat. Kebijakan tersebut juga harus memberikan peran yang relevan kepada lembaga dan departemen pemerintah yang akan memberikan arahan dan dukungan teknis, mereka yang akan memberikan visi reformasi tata kelola, dan prinsip dan pedoman proses umum (seperti Departemen Pendayagunaan Aparatur Negara yang perannya dalam upaya e-governance harus menjadi pusat, tetapi telah agak diredam sampai saat ini) dan departemen yang benar-benar melakukan kegiatan e-governance di bidang kompetensi dan pekerjaan masing-masing. Ini juga akan menyelaraskan e-governance dengan dorongan keseluruhan reformasi pemerintahan di India - terutama, desentralisasi, hak atas informasi, dan pemantauan masyarakat dan audit sosial, yang tujuan utamanya harus dilayani oleh e-governance. Kita perlu beralih dari e-governance prosedural - yang hanya mengotomatisasi dan mendigitalkan proses yang ada memberikan keuntungan yang efisien, sesuatu yang hampir merupakan proses alami di semua organisasi di seluruh dunia, untuk mengubah e-governance yang memiliki titik tolak dalam upaya khusus untuk mengatasi masalah tersebut. berbagai tantangan tata kelola dan proses reformasi di India.

Inisiatif kebijakan baru-baru ini yang menjanjikan adalah RUU Penyediaan Layanan Elektronik (EDS) yang saat ini ada di DPR. Undang-undang yang diusulkan ini mewajibkan semua lembaga pemerintah untuk mulai memberikan layanan mereka dalam mode elektronik. Semua layanan yang dapat diberikan secara elektronik harus disediakan. Ada ketentuan untuk Komisi EDS independen di tingkat pusat dan negara bagian yang akan memantau penyediaan layanan pengiriman elektronik. Undang-undang ini diharapkan dapat memberikan tekanan besar pada berbagai instansi pemerintah untuk segera menerapkan e-governance, dan karenanya merupakan langkah yang cukup positif.

Namun, RUU yang diusulkan hanya mendorong lembaga-lembaga menuju e-governance tanpa memberi tahu mereka bagaimana melakukannya, dan dengan tujuan inti apa yang dipikirkan. Akankah kebutuhan untuk mematuhi persyaratan legislatif, misalnya, membuat departemen cenderung untuk cepat mencari transfer tunai yang jauh lebih mudah dilakukan melalui infrastruktur penjangkauan berbasis TIK, bahkan ketika dijalankan oleh lembaga luar secara komersial, bahkan ketika layanan tertentu mungkin tidak paling cocok untuk mode transfer tunai? Dorongan yang disambut baik untuk penyerapan e-governance yang lebih cepat, seperti yang diharapkan disediakan oleh undang-undang EDS, membuatnya semakin penting untuk mengartikulasikan kebijakan e-governance secara keseluruhan di India, yang membuat pemeriksaan sosio-politik terperinci tentang kemungkinan-

kemungkinan baru dengan mempertimbangkan kebutuhan khusus dan dorongan reformasi pemerintahan saat ini di India.

2.5 INISIATIF PEMERINTAH PUSAT

Di India, dorongan utama untuk e-Governance diberikan oleh peluncuran NICNET pada tahun 1987 – jaringan komputer berbasis satelit nasional. Hal ini diikuti oleh peluncuran program Sistem Informasi Distrik Pusat Informatika Nasional (DISNIC) untuk mengkomputerisasi semua kantor distrik di negara yang menawarkan perangkat keras dan perangkat lunak gratis kepada Pemerintah Negara Bagian. NICNET diperluas melalui ibu kota negara bagian ke semua kantor pusat distrik pada tahun 1990. Pada tahun-tahun berikutnya, dengan komputerisasi yang berkelanjutan, konektivitas Tele dan konektivitas internet membentuk sejumlah besar inisiatif e-Governance, baik di tingkat Serikat dan Negara Bagian.

Perumusan Rencana e-Governance Nasional (NEGP) oleh Departemen Elektronika dan Teknologi Informasi (DEITY) dan Departemen Pendayagunaan Aparatur Negara dan Pengaduan Masyarakat (DAR&PG) pada tahun 2006 telah mendorong proses e-Governance.
Inisiatif Pusat meliputi:

- Rencana e-Governance Nasional (NEGP)
- Divisi e-Governance Nasional (NEGD)
- Infrastruktur e-Governance
- Proyek Mode Misi
- Layanan Warga
- Layanan Bisnis
- Layanan Pemerintah
- Proyek dan Inisiatif
- R&D dalam e-Governance
- Model RFP untuk Proyek e-Governance

2.6 INISIATIF PEMERINTAH NEGARA BAGIAN

Beberapa Pemerintah Negara Bagian telah mengambil berbagai langkah inovatif untuk mempromosikan e-Governance dan telah menyusun peta jalan untuk implementasi TI dan penyampaian layanan kepada warga secara online. Aplikasi yang telah diimplementasikan ditargetkan untuk menyediakan layanan Government to Citizen (G2C), Government to Business (G2B) dan Government to Government (G2G) dengan penekanan pada penggunaan bahasa lokal.

Setiap Negara Bagian memiliki fleksibilitas untuk mengidentifikasi hingga lima Proyek Modus Misi khusus Negara Bagian tambahan (relevan untuk pembangunan ekonomi di Negara Bagian). Dalam kasus di mana Bantuan Pusat diperlukan, penyertaan tersebut dipertimbangkan atas saran dari Kementerian/Departemen Lini terkait. Negara bagian memiliki MMP tentang Pertanian, Pajak Komersial, e-District, Pertukaran Ketenagakerjaan, Catatan Tanah, Kotamadya, Gram Panchayats, Polisi, Transportasi Jalan, Perbendaharaan, dll. Selain MMP, Amerika memiliki inisiatif e-Governance lainnya.

Tabel 2.1 Daftar layanan e-Governance

Wilayah Negara Bagian/Serikat	Inisiatif yang mencakup otomatisasi departemen, pengumpulan biaya pengguna, penyampaian informasi kebijakan/program, dan penyampaian hak
Andhra Pradesh	e-Seva, CARD, VOICE, MPHS, FAST, e-Cops, AP online—Toko serba ada di Internet, Saukaryam, Pemrosesan Transaksi Online
Bihar	Informasi Manajemen Administrasi Pajak Penjualan
Chhattisgarh	Chhattisgarh InfoTech Promotion Society, kantor Treasury, proyek e-linking
Delhi	Sistem Pelacakan Kendaraan Otomatis, Komputerisasi situs web kantor RCS, Sistem Izin Elektronik, Sistem Informasi Manajemen Pendidikan, dll
goa	Proyek Dharani
Gujarat	Mahiti Shakti, permintaan dokumen Pemerintah online, Buku formulir online, buku GR online, sensus online, pemberitahuan tender.
Haryana	Nai Disha
Himachal Pradesh	Lok Mitra
Karnataka	Bhoomi, Khajane, Kaveri
Kerala	e-Srinkhala, RDNet, Jaringan Cepat, Handal, Instan, Efisien untuk Penyaluran Layanan (TEMAN)
Madhya Pradesh	Gyandoot, Gram Sam park, Smart Card di Departemen Perhubungan, Komputerisasi MP Badan Pemasaran Pertanian Negara (Mandi Board) dll
Maharashtra	SETU, Sistem Manajemen Pengaduan Online—Mumbai
Rajasthan	Jan Mitra, Raj SWIFT, Lokmitra, RajNIDHI
Tamil Nadu	Rasi Maiyams–Kanchipuram; Formulir aplikasi yang terkait dengan utilitas publik, pemberitahuan tender, dan tampilan
Negara Bagian Timur Laut	
Arunachal Pradesh,	Pusat Informasi Masyarakat. Formulir tersedia di
Manipur, Meghalaya,	situs web Meghalaya di bawah skema yang terkait dengan
Mizoram & Nagaland	kesejahteraan sosial, persediaan makanan sipil dan urusan konsumen, transportasi perumahan dll.

Sumber: Artikel Quest PC

2.7 PROYEK E-GOVERNANCE DI INDIA

E-governance di Andhra Pradesh: Bagian situs web Andhra Pradesh ini menampilkan berbagai inisiatif dan aplikasi E-Governance yang diterapkan di negara bagian tersebut.

E-Governance di Kementerian/Departemen dan Pemerintah Negara Bagian Situs web Kementerian Teknologi Informasi (MIT), Pemerintah. India mencantumkan secara singkat

Prakarsa E-Governance yang dilakukan oleh berbagai Kementerian/Departemen dan Pemerintah Negara Bagian.

Gyandoot: Gyandoot adalah intranet di distrik Dhar Madhya Pradesh, menghubungkan warnet pedesaan yang melayani kebutuhan sehari-hari masyarakat. Situs web ini merupakan perpanjangan dari intranet Gyandoot, untuk memberikan akses global. Situs ini menawarkan layanan berikut: Sistem Informasi Pemasaran Komoditas/ Mandi; Fotokopi khasra, B1/khatauni dan peta; Pendaftaran aplikasi online; Sertifikat Penghasilan; Surat Keterangan Domisili (mool niwasi); Sertifikat Kasta; Buku tabungan pemilik tanah tentang hak dan pinjaman tanah (Bhoo adhikar evam rin pustika). Warana: Tujuan utama dari proyek Wired Village yang baru-baru ini diluncurkan adalah untuk mendemonstrasikan penggunaan infrastruktur TI yang efektif dalam percepatan pembangunan sosial-ekonomi 70 desa di sekitar Warana Nagar di distrik Kolhapur dan Sangli di negara bagian Maharashtra. Struktur koperasi yang ada telah digunakan bersama dengan VSAT kecepatan tinggi untuk memungkinkan akses Internet ke koperasi yang ada. Proyek ini bertujuan untuk memberikan informasi pertanian, medis, dan pendidikan kepada penduduk desa dengan mendirikan stan fasilitasi jaringan di desa-desa.

E-Governance di kota Noida: Compaq India telah bergandengan tangan dengan Electronics Research and Development Center of India (ERDCI), Noida, untuk mendirikan pusat kompetensi yang akan memungkinkan e-governance di kota Noida dan berbagai negara bagian lainnya. Warga akan dapat membayar tagihan listrik dan telepon, mengajukan pengembalian IT, mendaftarkan pernikahan dan kematian, antara lain di kios informasi yang terletak di kota. Setelah proyek beroperasi penuh, warga dapat membayar utilitas, mendapatkan ganti rugi keluhan, dan berbagai pekerjaan penting lainnya melalui kios info ini.

"RajNidhi": Kios informasi : "RajNidhi" adalah sistem kios informasi berkemampuan web yang dikembangkan bersama oleh Departemen Teknologi Informasi negara bagian Rajasthan dan Badan Layanan Komputer (RajComp) Negara Bagian Rajasthan.

Sebelumnya pada tanggal 23 Maret 2000, Nayla menjadi desa pertama di Rajasthan yang memiliki "Kios Informasi Raj Nidhi" ketika Presiden AS, Mr. Bill Clinton mengunjungi desa ini untuk mengamati berfungsinya Gram Panchayat.

"raj-SWIFT": Intranet pemerintah Rajasthan: Departemen Teknologi Informasi (DoIT) Negara Bagian Rajasthan telah mengembangkan Intranet milik Pemerintah yang disebut sebagai "raj-SWIFT". SWIFT di sini adalah singkatan dari Statewide Intranet on Fast Track. Sistem yang dibangun dengan menggunakan teknologi dan perangkat Internet ini akan memfasilitasi komunikasi data, teks dan email online antara kantor Ketua Menteri dan semua 32 Kolektor Distrik secara satu-ke-satu, sehingga membawa Ketua Pelaksana Administrasi negara bagian dan distrik cukup dekat hanya dengan satu klik mouse.

Mekanisme Sistem Izin Satu Jendela: Untuk mengatasi waktu yang sangat lama yang diperlukan untuk mendapatkan persetujuan/lisensi undang-undang, dll. dari berbagai departemen/lembaga pemerintah, Biro Promosi Industri & Kantor Komisaris (Investasi & NRI), Pemerintah Rajasthan, telah memperkenalkan Sistem Izin Satu Jendela melalui Formulir Aplikasi Komposit Tunggal.

E-Governance di Panchayats di Kerala: Situs web departemen Reformasi Administrasi dan Keluhan Publik, Kementerian Personalia, Keluhan Publik dan Pensiun menampilkan artikel tentang inisiatif e-governance yang diadopsi oleh Panchayats di Kerala.
E-Governance di Himanchal Pradesh: Himanchal Pradesh untuk fokus pada layanan IT & e-governance, yang akan mencakup transkripsi medis, call center, pemrosesan data, operasi back office dan GIS.

Paket untuk Proyek Administrasi Undang-Undang Pendaftaran yang Efektif di Kerala: Pemerintah Kerala telah meluncurkan proyek berjudul PEARL (Paket untuk Administrasi yang Efektif dari Undang-Undang Pendaftaran) untuk komputerisasi Departemen Pendaftaran di Negara Bagian.

Pusat E-Governance di Sekretariat Haryana: Pemerintah Haryana telah mendirikan pusat e-governance di Sekretariat untuk memantau teknologi informasi di negara bagian secara efektif.

Jaringan Pengetahuan Nasional: NKN adalah jaringan pan-India multi-gigabit canggih untuk menyediakan tulang punggung jaringan berkecepatan tinggi terpadu untuk semua lembaga terkait pengetahuan di negara ini. Tujuan dari jaringan pengetahuan seperti itu menuju ke inti dari pencarian negara untuk membangun institusi berkualitas dengan fasilitas penelitian yang diperlukan dan menciptakan kumpulan profesional yang sangat terlatih. NKN akan memungkinkan para ilmuwan, peneliti dan mahasiswa dari berbagai latar belakang dan geografi yang beragam untuk bekerja sama untuk memajukan pembangunan manusia di daerah kritis dan berkembang.

Fitur

NKN dirancang sebagai jaringan Smart Ultra High Bandwidth yang secara mulus menghubungkan institusi Ilmiah dan Teknologi terkemuka - yang mengejar penelitian dan pengembangan kelas dunia. Desain NKN pada dasarnya bersifat proaktif; itu memperhitungkan persyaratan yang mungkin terjadi dalam waktu dekat dan jangka panjang. Beberapa fitur yang menonjol dari NKN adalah:

- Membangun Konektivitas untuk Pengetahuan dan berbagi informasi.
- Mengaktifkan Penelitian Kolaboratif di bidang-bidang yang sedang berkembang seperti Pemodelan Iklim.
- Memfasilitasi pendidikan jarak jauh di bidang khusus seperti kedokteran, bidang teknologi tinggi yang sedang berkembang meliputi teknologi info-bio-nano.
- Memfasilitasi tulang punggung e-governance berkecepatan sangat tinggi untuk berbagi informasi.

NKN juga akan bertindak sebagai test bed untuk penelitian di bidang jaringan, keamanan dan model pengiriman untuk berbagai layanan. Karena NKN adalah prakarsa baru, ia akan memanfaatkan prakarsa yang ada, untuk memastikan peluncuran lebih cepat dengan investasi sederhana.

Jasa

Jaringan NKN dirancang dengan tujuan untuk menyediakan:

- Tingkat ketersediaan tertinggi
- Konektivitas yang kuat & andal

- Tingkat Skalabilitas tertinggi (direncanakan secara khusus agar sesuai dengan tuntutan masa depan yang tidak diketahui yang tidak dapat dibayangkan saat ini)
- Kapasitas Bandwidth Terbaik: Untuk NKN, berbagai National Long Distance Carriers (NLDs) telah menyediakan link kapasitas 1Gbps / 2.5Gbps yang dapat disembuhkan sendiri. Selanjutnya, NLD sedang dalam proses peningkatan (menggunakan DWDM) ke konektivitas 10Gbps atau lebih.

Layanan utama NKN dapat dikategorikan secara luas di bawah judul berikut:

- Layanan Umum: Internet, Intranet, Tampilan Manajemen Jaringan, Email, Gateway Pesan, Gateway Caching, Sistem Nama Domain, Hosting Web, Voice over IP, Layanan Multipoint Control Unit (MCU), Portal Video, SMS Gateway, Lokasi Bersama Layanan, Streaming Video, dll.
- Layanan Komunitas: Penyimpanan Bersama, Aplikasi Perangkat Lunak Daftar Email (LISTSERV), Layanan Otentikasi, EVO, Session Initiation Protocol (SIP), Layanan Kolaborasi, Layanan Pengiriman Konten, Kolaborasi Internasional dengan EU-India Grid, Jaringan Dering Global untuk Aplikasi Tingkat Lanjut Pengembangan (GLORIAD)dll.
- Layanan Khusus: Layanan Penggabungan Jaringan Pribadi Virtualu

2.8 STANDAR E-GOVERNANCE

Untuk memastikan Interoperabilitas antara aplikasi e-Governance, Pemerintah India telah menyiapkan mekanisme kelembagaan untuk perumusan Standar melalui upaya kolaboratif pemangku kepentingan dari DIT, NIC, STQC, Departemen Pemerintah lainnya, Industri, Akademisi dan Publik. Berbagai kelompok kerja dan komite ahli telah dibentuk untuk tujuan ini. NIC memainkan peran kunci dalam koordinasi dan mengarahkan proses perumusan standar dan juga partisipasi teknis dalam persiapan makalah Pendekatan, perumusan standar, proses peninjauan draf dan POC.

Kebijakan tentang Standar Terbuka, Standar Metadata dan Data untuk Identifikasi Orang & Kodifikasi Wilayah Tanah, Standar Data Biometrik untuk Gambar Sidik Jari dan Wajah, Pedoman Interoperabilitas untuk Sertifikat Tanda Tangan Digital, Pedoman penggunaan Tanda Tangan Digital, Standar Pengkodean dan Huruf Bahasa India, Kerangka Jaminan Kualitas , dokumen Persyaratan Penilaian Kesesuaian, Kerangka Kerja dan Pedoman Keamanan Informasi telah dipublikasikan di portal (http://egovstandards.gov.in). Standar untuk desain e-Formulir, Kerangka Interoperabilitas untuk e-Governance di India, Standar teknis di bidang Interoperabilitas sedang dalam tahap persiapan lanjutan.

Standar yang Diberitahukan

Standar Biometrik:
Standar Data Gambar Wajah Ver1.0
Standar Data Gambar Sidik Jari Ver1.0
Standar Data Gambar Iris Ver1.0
Persyaratan Penilaian Kesesuaian (CARE)
Persyaratan Penilaian Kesesuaian untuk Aplikasi e-Governance Ver.1.0
Presentasi tentang Tinjauan Dokumen CARE Ver.1.0
Standar Pelestarian Digital:

Standar E-Governance untuk Informasi Pelestarian Dokumentasi e-Records Ver1.0 (Metadata & Skema)
Standar E-Governance untuk Informasi Pelestarian Dokumentasi e-Records Ver1.0 (XSD)
Standar Teknologi Lokalisasi & Bahasa:
Pengkodean Karakter: Standar Ver1.0
Font: Standar Ver.1.0
Metadata dan Standar Data:
Demografi MDDS Ver. 1.1
Kerangka Penjaminan Mutu:
Ringkasan Presentasi Dokumen QAF Ver.1.0 QualityAssuranceFramework Ver.1.0
Standar Teknis untuk IFEG:
Standar Teknis untuk IFEG Ver1.0

Pedoman

Tanda tangan digital:
Interoperabilitas Sertifikat Tanda Tangan Digital Ver2.0 Penggunaan Tanda Tangan Digital dalam e-Governance Ver1.0 Pelestarian Digital:
Praktik Terbaik dan Pedoman untuk Produksi Perceivable e-Records Ver1.0 Situs web Pemerintah India:
Keamanan Informasi Pedoman Web GOI:
ESAFE-GD210-Pedoman Implementasi ver1.0
ESAFE-GD220-Pedoman Penilaian ver1.0
Ikhtisar ESAFE
Makalah Pendekatan Kerangka ESAFE Ver1.0
ESAFE GD100 IS Pedoman untuk Kategorisasi Keamanan Sistem Informasi Ver1.0
Katalog Kontrol Keamanan ESAFE GD200 Ver1.0
ESAFE GD201 Kontrol Keamanan Dasar Sistem Informasi Berdampak Rendah Ver1.0
ESAFE GD202 Kontrol Keamanan Dasar Sistem Informasi Dampak Menengah Ver1.0
ESAFE GD203 Kontrol Keamanan Dasar Sistem Informasi Berdampak Tinggi Ver1.0
Pedoman ESAFE GD300 untuk Penilaian Risiko Keamanan Informasi dan mgmt Ver1.0
Lokalisasi Aplikasi e-Governance dalam Bahasa India:
Praktik Terbaik untuk Lokalisasi Aplikasi e-Governance dalam Bahasa India Ver5.7
Pedoman E-Procurement:
Kepatuhan terhadap Persyaratan Kualitas Sistem e-Procurement Mobile Governance:
Pedoman Saluran Pengiriman Penyediaan Layanan Publik Melalui Perangkat Seluler
Praktik Terbaik untuk Lokalisasi Aplikasi Web Seluler dalam Bahasa India

2.9 LAYANAN WEB

NIC memperluas layanan World Wide Web yang komprehensif (http://webservices.nic.in) ke Pemerintah Pusat dan Negara Bagian, Kementerian & Departemen di bidang konsultasi, desain dan pengembangan web, hosting web, layanan web bernilai tambah untuk promosi situs web , peningkatan situs web & pelatihan. Infrastruktur hosting disediakan untuk sejumlah besar proyek e-governance seperti CGHS, Portal

Panchayats, akuntansi Pemerintah, Portal Hasil Ujian, Konseling Online hingga Penerimaan ke berbagai kursus profesional di seluruh negeri.

Berbagai layanan hosting NIC dimulai langsung dari Hosting Berbagi Pakai dan Server Khusus hingga Server Lokasi Bersama dan Hosting Terkelola. Solusi hosting tersedia di berbagai platform seperti Linux, Windows dan Solaris dll. NIC juga mendukung teknologi web tercanggih dan berbagai database di server. Infrastruktur hosting mencakup sejumlah besar kinerja kuat yang disetel dan server yang aman. Solusi penyeimbangan beban dan pengelompokan digunakan untuk mengelola lalu lintas padat di situs web secara efektif selama jam sibuk dan untuk memastikan ketersediaan tingkat tinggi. Sebuah situs yang dibawa ke NIC untuk hosting dapat berada di server dalam waktu kurang dari satu jam. Mengembangkan kehadiran yang sukses di web membutuhkan kombinasi konten berkualitas, pemrograman dinamis, grafik yang kuat, dan yang terpenting, strategi promosi yang direncanakan dengan cermat. NIC membantu menyempurnakan situs sedemikian rupa sehingga mendapat peringkat tinggi di berbagai mesin pencari. Situs juga dipromosikan melalui portal NIC sendiri seperti "India Image" dan "GOI-Directory" yang menarik banyak pengunjung setiap hari dari seluruh dunia.

- URL:
  http://webservices.nic.in
- Rincian Kontak
  Pusat Data dan Divisi Layanan Web Pusat Informatika Nasional Blok A, Kompleks CGO Jalan Lodhi, New Delhi-110003, Email:-nic-web support [at]lsmgr[dot]nic[dot]in.Phone:011-2430536

2.10 RINGKASAN

E-governance adalah fitur yang sangat penting dari pemerintahan. Dalam unit ini konsep sejarah e-governance di India, asal e-governance di India melalui Pusat Informatika Nasional, rencana E-Governance Nasional, inisiatif Pemerintah Pusat, inisiatif Pemerintah Negara Bagian, berbagai proyek e-governance penting di India, Jaringan Pengetahuan Nasional, jaringan e-governance dan e-services dibahas panjang lebar untuk pemahaman dengan bantuan berbagai contoh terkait dan inisiatif dari pemerintah untuk memperkuat sektor ini untuk kepentingan warga.

2.11 BEBERAPA BUKU BERGUNA

20. Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
21. Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
22. Cyber Crime dan Cyber Terrorism oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
23. Terorisme Cyber oleh S. Venkatesh (Penulis)
24. Keamanan Crypto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
25. Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)

26. Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
27. Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
28. Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
29. Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
30. Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
31. Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
32. Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
33. Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
34. Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
35. Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
36. Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
37. Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
38. Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

2.12 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah?

1. Munculnya e-governance telah menjadi salah satu perkembangan web yang paling mencolok.
2. Digitalisasi catatan kepemilikan dan transaksi tanah telah menjadi salah satu bidang utama dengan dampak yang cukup besar.
3. NIC menyediakan infrastruktur TIK umum nasional untuk mendukung layanan e-governance kepada warga.
4. Jaringan Pengetahuan Nasional adalah jaringan multi gigabit pan India canggih untuk menyediakan jaringan kecepatan tinggi terpadu.
5. Sebuah situs yang dibawa ke NIC untuk hosting dapat berada di server dalam waktu kurang dari satu jam.

B. Isi Bagian yang Kosong:

1. Di antara negara-negara berkembang ..... telah menjadi adaptor awal e-governance.
2. Bangsa; Pusat Informatika (NIC) didirikan pada.....
3. Inisiatif kebijakan baru-baru ini yang menjanjikan di..... Biff yang ada di Parlemen saat ini.
4. DISNIC artinya.....
5. NIC memperluas ..... yang komprehensif kepada Pemerintah Pusat dan Negara Bagian.

2.13 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. India
2. 1976
3. Pengiriman Layanan Elektronik (EDS)
4. Sistem Informasi Daerah Pusat Informatika Nasional
5. Layanan World Wide Web

2.14 PERTANYAAN TERMINAL

a. Bagaimana sejarah e-governance di india?
b. Apa itu Rencana E-governance Nasional?
c. Membahas secara rinci inisiatif Pemerintah Pusat dan Negara Bagian dengan mengacu pada e-governance.
d. Tulis catatan di Jaringan Pengetahuan Nasional.
e. Tulis catatan tentang Standar E-Governance dan E-Services.

BAB 3
NETRALITAS BERSIH

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan Netralitas Bersih
- Memahami dimensi internasional Netralitas Bersih
- Memahami masalah teknis dan hukum terkait Netralitas Bersih

3.1 PENGANTAR

Netralitas bersih (juga netralitas jaringan, netralitas Internet, atau kesetaraan bersih) adalah prinsip bahwa penyedia layanan Internet dan pemerintah harus memperlakukan semua data di Internet secara setara, tidak membeda-bedakan atau membebankan biaya secara berbeda berdasarkan pengguna, konten, situs, platform, aplikasi, jenis lampiran peralatan, atau cara komunikasi. Istilah ini diciptakan oleh profesor hukum media Universitas Columbia Tim Wu pada tahun 2003 sebagai perpanjangan dari konsep lama dari pembawa umum.

Ada perdebatan luas tentang apakah netralitas bersih harus diwajibkan oleh hukum, khususnya di Amerika Serikat. Perdebatan tentang masalah netralitas bersih mendahului penciptaan istilah tersebut. Pendukung netralitas bersih seperti Lawrence Lessig telah menyuarakan keprihatinan tentang kemampuan penyedia broadband untuk menggunakan infrastruktur jarak jauh mereka untuk memblokir aplikasi dan konten Internet (misalnya situs web, layanan, dan protokol), dan bahkan untuk memblokir pesaing.

Pendukung netralitas mengklaim bahwa perusahaan telekomunikasi berusaha untuk memaksakan model layanan berjenjang untuk mengontrol saluran pipa dan dengan demikian menghilangkan persaingan, menciptakan kelangkaan buatan, dan mewajibkan pelanggan untuk membeli layanan mereka yang tidak kompetitif. Banyak yang percaya netralitas bersih menjadi sangat penting sebagai pelestarian kebebasan saat ini. Pendukung utama netralitas bersih termasuk Vinton Cerf, salah satu penemu Internet Protocol, dan Tim Berners-Lee, pencipta Web.

Contoh pelanggaran netralitas bersih termasuk ketika penyedia layanan internet, Comcast, dengan sengaja memperlambat komunikasi peer-to-peer. Pada tahun 2007, satu perusahaan lain menggunakan inspeksi paket mendalam untuk mendiskriminasi peer-to-peer, protokol transfer file, dan game online, melembagakan sistem penagihan kelebihan penggunaan gaya ponsel, layanan nilai tambah free-to-telecom, dan bundling . Kritik netralitas bersih berpendapat bahwa diskriminasi data diinginkan untuk alasan seperti menjamin kualitas layanan. Bob Kahn, salah satu penemu Internet Protocol, menyebut istilah netralitas bersih sebagai slogan dan menentang penetapannya, tetapi dia mengakui bahwa dia menentang fragmentasi jaringan setiap kali hal ini mengecualikan peserta lain.

3.2 NETRALITAS BERSIH: ARTI DAN CAKUPAN

Netralitas bersih adalah ide yang diturunkan dari cara kerja saluran telepon sejak awal abad ke-20. Dalam hal saluran telepon, Anda dapat menghubungi nomor apa pun dan menyambungkannya. Tidak masalah jika Anda menelepon dari operator A ke operator B. Tidak masalah jika Anda menelepon restoran atau pengedar narkoba. Operator tidak memblokir akses ke nomor atau sengaja menunda koneksi ke nomor tertentu, kecuali dipaksa oleh hukum. Sebagian besar negara memiliki aturan yang meminta operator telekomunikasi untuk menyediakan layanan telepon tanpa filter dan tidak terbatas. Ketika internet mulai lepas landas pada 1980-an dan 1990-an, tidak ada aturan khusus yang meminta penyedia layanan internet (ISP) untuk mengikuti prinsip yang sama. Tapi, kebanyakan karena operator telekomunikasi juga ISP, mereka menganut prinsip yang sama. Prinsip ini dikenal sebagai netralitas bersih. ISP tidak mengontrol lalu lintas yang melewati servernya. Ketika pengguna web terhubung ke situs web atau layanan web, dia mendapatkan kecepatan yang sama. Kecepatan data untuk video YouTube dan foto Facebook secara teoritis sama. Pengguna dapat mengakses situs web atau layanan web legal apa pun tanpa campur tangan dari ISP.

Netralitas Jaringan (atau netralitas "bersih") adalah konsep non-diskriminasi online. Merupakan prinsip bahwa konsumen/warga negara harus bebas untuk mendapatkan akses ke - atau menyediakan - konten dan layanan Internet yang mereka inginkan, dan akses konsumen tidak boleh diatur berdasarkan sifat atau sumber konten atau layanan tersebut. Penyedia informasi - yang mungkin berupa situs web, layanan online, dll., dan yang mungkin berafiliasi dengan perusahaan komersial tradisional tetapi juga mungkin merupakan warga negara perorangan, perpustakaan, sekolah, atau entitas nirlaba - pada dasarnya harus memiliki kualitas akses yang sama untuk mendistribusikan informasi mereka. persembahan. Pemilik "pipa" (operator) tidak boleh menagih beberapa penyedia informasi lebih banyak uang untuk pipa yang sama, atau membuat kesepakatan eksklusif yang menurunkan semua orang (termasuk entitas nonkomersial atau startup kecil) ke "jalur lambat" Internet. Prinsip ini harus berlaku bahkan ketika penyedia broadband menyediakan pengangkutan Internet ke pesaing. Netralitas bersih adalah prinsip dasar Internet. Ini adalah prinsip yang menggabungkan kedua undang-undang "operator umum" yang telah lama mengatur saluran telepon yang digunakan untuk telepon suara dan akses dial up. Sekarang, banyak konsumen menerima layanan broadband melalui teknologi lain (kabel, DSL) yang tidak tunduk pada persyaratan common-carriage yang sama. Meskipun teknologi ini tidak diragukan lagi lebih unggul daripada dial-up, kurangnya prinsip netralitas bersih yang dapat diterapkan menjadi perhatian kami. Perusahaan kabel dan DSL berencana untuk terlibat dalam "diskriminasi kecil" dengan menyediakan koneksi yang lebih cepat ke situs web dan layanan yang membayar mahal, atau dengan memilih mitra bisnis mereka sendiri saat mengirimkan konten. Saat Internet bergerak maju, apakah benar-benar bijaksana untuk meninggalkan netralitas bersih?

3.3 ARGUMEN UNTUK NETRALITAS BERSIH

Namun, para pendukung netralitas bersih terbagi atas pertanyaan apakah Internet adalah barang publik atau tidak dan apakah akses ke Internet harus menjadi hak fundamental atau tidak. Salah satu argumen utama yang mendukung menjadikan akses Internet sebagai hak fundamental adalah bahwa ia menyediakan platform penting bagi hak-hak lain seperti

kebebasan berbicara, kebebasan pers, dan kebebasan berkumpul. Hal ini sangat relevan mengingat keberadaan Internet di semua aspek kehidupan modern dan lintas platform. Internet telah dibandingkan dengan jaringan listrik untuk menekankan pentingnya inovasi dan kemajuan di abad ke-21, dengan saran bahwa jika jaringan listrik tidak netral, banyak yang akan dihargai di luar sains dan penemuan.

Setiap upaya untuk membawa Internet di bawah peraturan pemerintah yang lebih ketat dapat dianggap sebagai penjangkauan pemerintah, terutama jika undang-undang tersebut ditulis untuk teknologi yang lebih tua. Pertanyaan tentang bagaimana mengklasifikasikan broadband - sebagai layanan informasi, layanan telekomunikasi, layanan kabel, atau utilitas publik - telah mengganggu perdebatan netralitas bersih. Gagasan tentang kendali pemerintah atas Internet sangat sensitif mengingat kontroversi baru-baru ini seputar pengumpulan intelijen. Masalah ini semakin rumit karena Internet sendiri tidak memiliki pemilik, tetapi berbagai komponen perangkat keras dan perangkat lunak Internet dimiliki oleh pihak yang berbeda dengan hak kekayaan intelektual tertentu. Perusahaan bebas adalah prinsip lain yang harus dihadapi. Penyedia layanan Internet (ISP) telah membayar untuk mengembangkan dan memelihara infrastruktur yang menyediakan Internet, dan bandwidth mahal. ISP berpendapat bahwa mereka harus dapat menutup biaya tersebut dengan membebankan biaya kepada mereka yang menggunakan lebih banyak. Beberapa tipe data - contoh yang menonjol adalah layanan streaming video - mengkonsumsi lebih banyak bandwidth daripada yang lain, dan karena itu ISP harus menanggung biaya tersebut; pilihan mereka adalah membebankan biaya lebih kepada konsumen atau membebankan biaya kepada penyedia konten untuk transmisi data.

Satu masalah dengan argumen ini, terutama di negara berkembang, adalah bahwa banyak ISP juga memiliki kepentingan bisnis lain, dan potensi konflik dan sensor muncul. Jika ISP juga menyediakan layanan panggilan internasional, maka masuk akal jika ISP tidak menganjurkan penggunaan Skype; jika mereka menyediakan layanan siaran video, mengapa mempromosikan streaming online? Terutama di negara berkembang, di mana konten semakin banyak disediakan secara online daripada melalui media 'tradisional', ada risiko konten dikendalikan oleh para penjaga gerbang Internet. Banyak penggunaan Internet di pasar berkembang dan berkembang terjadi di ponsel. Hal ini telah mendorong operator untuk bekerja sama dengan penyedia konten untuk membuat rencana akses internet terbatas, yang disebut 'taman bertembok'.

Google Free Zone dan Face book Zero adalah dua contohnya, di mana pelanggan dari jaringan yang berpartisipasi dapat menggunakan layanan Google atau Face book terbatas secara gratis. Paket ini mungkin ditawarkan sebagai cara untuk menarik pelanggan agar menggunakan lebih banyak data, dan dengan demikian pindah ke paket yang lebih mahal. Ini adalah pertaruhan yang mahal bagi penyedia jaringan, karena Facebook setidaknya tidak menanggung biaya data gratis, yang berarti penyedia jaringan harus melakukannya. Namun, penyedia jaringan membutuhkan layanan konten ini, karena semakin menarik pelanggan daripada paket suara dan teks tradisional. India saat ini tidak memiliki undang-undang tentang netralitas bersih, dan Otoritas Regulasi Telekomunikasi India, meskipun pada prinsipnya mendukung non-diskriminasi, saat ini tidak menegakkannya. Sementara secara umum ISP India mematuhi prinsip netralitas bersih, ada beberapa jenis lalu lintas tertentu yang

diperlambat oleh ISP India, tanpa sepengetahuan pelanggan. TRAI telah mencatat pentingnya netralitas bersih dan risiko ISP yang mengendalikan konten dalam makalah konsultasi tahun 2006. Vodafone India, Airtel, Aircel, dan penyedia lainnya telah menunjukkan keinginan untuk perjanjian pembagian pendapatan dengan penyedia konten seperti YouTube dan Face book, pandangan yang juga dibagikan oleh Asosiasi Operator Seluler India (COAI).

Mahkamah Agung India memutuskan dalam LIC v Manubhai D Shah bahwa Pasal 19(1)(a) - hak atas kebebasan berbicara dan berekspresi - memerlukan lingkungan publik yang inklusif, mengikuti argumen bahwa kebebasan berbicara yang dijamin secara konstitusional tidak banyak berguna jika dibatasi oleh pihak swasta. Jika pihak-pihak berpengaruh dapat menekan pesaing yang lebih kecil ke jalur Internet yang lebih lambat, mereka memperoleh kemampuan untuk membungkam perdebatan dan mengendalikan pandangan secara tidak demokratis. Analis telah menyarankan bahwa melindungi kebebasan berbicara adalah salah satu argumen terbaik untuk netralitas bersih di India. Dengan India yang berusaha menghubungkan miliaran berikutnya, dan menjadi pemain kunci dalam debat Internet global, penting untuk membentuk kebijakan domestik dengan jelas. Kombinasi kepentingan regulasi, oposisi perusahaan dan hak konstitusional menunjukkan bahwa waktu yang tepat untuk debat bernuansa netralitas bersih di India, dengan regulasi akhirnya menyeimbangkan kebutuhan penyedia dan konsumen yang keduanya semakin bergantung pada Internet.

Asosiasi Perpustakaan Amerika adalah pendukung kuat untuk kebebasan intelektual, yang merupakan "hak semua orang untuk mencari dan menerima informasi dari semua sudut pandang tanpa batasan." Kebebasan intelektual sangat penting bagi demokrasi kita, karena kita mengandalkan kemampuan orang untuk memberi tahu mereka. Internet menghubungkan orang-orang dari beragam asal geografis, politik, atau ideologis, sangat meningkatkan kemampuan setiap orang untuk berbagi dan menginformasikan diri mereka sendiri dan orang lain. Komitmen lama perpustakaan terhadap kebebasan berekspresi di ranah konten sudah dikenal luas; dalam konteks debat netralitas bersih, bagaimanapun, kami percaya sama pentingnya untuk menekankan bahwa kebebasan perpustakaan dan pustakawan untuk menyediakan jenis layanan informasi baru yang inovatif akan menjadi pusat pertumbuhan dan perkembangan budaya demokrasi kita. Dunia di mana pustakawan dan perusahaan non-komersial lainnya terbatas pada "jalur lambat" Internet sementara film definisi tinggi dapat memperoleh perlakuan istimewa tampaknya bagi kita mengabaikan prioritas utama bagi masyarakat demokratis - kebutuhan untuk memungkinkan pendidik, pustakawan , dan, pada kenyataannya, semua warga negara untuk menginformasikan diri mereka sendiri dan satu sama lain sebanyak yang dapat diinformasikan oleh kepentingan komersial dan media utama kepada mereka. Kemampuan Internet untuk menyebarkan dan berbagi ide semakin baik. Dengan teknologi modern, individu dan kelompok kecil dapat menghasilkan sumber daya audio dan video yang kaya yang dulunya merupakan domain eksklusif perusahaan besar. Kita harus bekerja untuk memastikan bahwa sumber daya ini tidak diturunkan ke pengiriman kelas dua di Internet – atau kebebasan intelektual yang dipupuk oleh Internet akan dibatasi. Salah satu aplikasi yang terutama diinvestasikan oleh perpustakaan adalah pembelajaran jarak jauh. Kelas yang ditawarkan menggunakan audio dan video yang dialirkan melalui Internet memiliki potensi besar untuk menghadirkan guru ahli ke rumah siswa di seluruh dunia.

3.4 ARGUMEN MENENTANG NETRALITAS BERSIH

Netralitas bersih memiliki pendukung dan penentangnya, dan saya tidak memiliki ruang di sini untuk membahas perselisihan itu. Dalam bentuknya yang paling luas dan absolut, netralitas bersih sangat kontroversial (termasuk argumen bahwa status quo yang ada tidak netral dalam arti sebenarnya). Namun, saya menganggap bahwa beberapa bentuk netralitas bersih merupakan tujuan yang penting dan diinginkan. Secara khusus, manipulasi informasi yang disengaja yang tersedia untuk pengguna internet – terutama untuk tujuan politik.

Contoh netralitas bersih dalam praktiknya adalah Perintah Internet Terbuka Komisi Komunikasi Federal Amerika tahun 2010, yang menjadi subjek litigasi dalam Verizon v. FCC yang baru-baru ini diselesaikan. Perintah Open Internet memberlakukan kewajiban transparansi, tidak ada pemblokiran, dan tidak ada diskriminasi yang tidak masuk akal, kepada penyedia layanan internet. Persyaratan kedua dan ketiga dikosongkan oleh Pengadilan Banding Amerika Serikat. Alasan untuk keputusan Pengadilan adalah bahwa ISP tidak dapat disamakan, dalam hukum, untuk "operator umum". Pengangkut umum adalah entitas yang menawarkan untuk mengangkut orang dan/atau barang dengan imbalan biaya (misalnya, perusahaan pelayaran, atau perusahaan bus). Operator umum dilisensikan untuk menjadi satu, dan seringkali, salah satu syarat untuk lisensi adalah kewajiban untuk tidak melakukan diskriminasi. Artinya, pengangkut umum tidak dapat menolak untuk mengangkut orang yang bersedia dan mampu membayar biaya yang diperlukan, tanpa adanya alasan yang memaksa (misalnya, jika orang tersebut menginginkan pengangkut untuk mengangkut selundupan). Pendukung netralitas bersih telah lama menyerukan untuk memperlakukan ISP sebagai operator umum, sebuah proposisi – seperti yang diamati di atas – ditolak oleh Pengadilan.

3.5 DISKRIMINASI DATA

Sementara prinsip dasar diskriminasi data adalah penyensoran, mereka yang mendukung praktik ini mengklaim bahwa ada manfaatnya. ISP adalah bisnis, dan dengan demikian, "... nyatakan dengan benar bahwa kendala eksternal yang tidak didorong oleh pasar pada kemampuan mereka untuk melakukan diskriminasi harga dapat berdampak buruk pada insentif mereka untuk berinvestasi dalam infrastruktur broadband dan kemampuan mereka untuk menutup investasi itu." Ada kalanya masuk akal, di mata ISP, untuk memberikan preferensi pada satu jenis konten di atas yang lain. Misalnya, memuat situs web teks dan gambar biasa tidak seberat memuat situs seperti Hulu dan Youtube. Frieden menyatakan bahwa "Beberapa Penyedia Layanan Internet (ISP) berusaha untuk mendiversifikasi Internet dengan memprioritaskan aliran bit dan dengan menawarkan jaminan kualitas layanan yang berbeda. Untuk beberapa pengamat, strategi ini merupakan diskriminasi berbahaya yang melanggar tradisi netralitas jaringan dalam switching, routing dan transmisi tra``i Internet].' Sementara argumen QoS adalah bahwa aturan netralitas jaringan memungkinkan pemilik jaringan untuk mempraktekkan beberapa jenis diskriminasi untuk melindungi fungsi jaringan.

Mereka yang menentang diskriminasi data mengatakan bahwa hal itu merugikan pertumbuhan Internet, serta ekonomi yang mengakar ke kedalaman model Internet.

“Alih-alih mempromosikan persaingan, pemilihan pemenang dan pecundang seperti itu akan melumpuhkan ekonomi. “Jika, misalnya, operator jaringan telekomunikasi memblokir paket data layanan Voice-over-IP yang mungkin menggantikan layanan telepon mereka

sendiri, ini tidak hanya akan mendiskriminasi perusahaan tertentu, tetapi juga mengurangi persaingan dan kesejahteraan ekonomi. Secara teknis, ini tidak akan menjadi masalah. Meskipun paket data homogen dalam hal switching dan perlakuan transmisi, jenis, sumber, dan tujuan dapat diungkapkan dan paket data ditangani secara berbeda jika operator jaringan lebih suka melakukannya. Masalah lain adalah bahwa jenis data yang diberikan perlakuan istimewa tergantung pada kebijaksanaan ISP. Ini memungkinkan mereka untuk memindahkan data sesuai keinginan mereka, apakah itu melalui "lensa" politik, moral, atau jenis "lensa" lainnya. Ini bertentangan dengan amandemen pertama, kebebasan berbicara karena dengan menghentikan jenis informasi tertentu dari mencapai pengguna akhir, mereka menyensor konten. Bukan tempat ISP untuk menyensor konten dari orang-orang.

Ancaman nyata terhadap Internet terbuka adalah di jaringan lokal (ujung), di mana pemilik jaringan dapat memblokir informasi yang masuk dari antar-jaringan, tetapi juga di jaringan lokal di mana kerugian paling besar dapat terjadi. Karena itu, aturan netralitas jaringan memungkinkan beberapa diskriminasi oleh jaringan lokal untuk melindungi dirinya sendiri, meskipun mungkin tidak didasarkan pada konten atau jenis aplikasi. Misalnya, pemilik jaringan ingin melindungi jaringannya agar tidak rusak. Jadi, beberapa diskriminasi diperbolehkan untuk "mencegah kerusakan fisik pada Jaringan Broadband lokal yang disebabkan oleh lampiran jaringan atau penggunaan jaringan apa pun." Ini berarti bahwa operator jaringan lokal tidak boleh mengontrol jenis aplikasi yang dipilih pengguna untuk digunakan, jenis perangkat apa yang digunakan pengguna untuk mengakses jaringan, atau jenis konten legal yang dipilih untuk disampaikan atau dikonsumsi pengguna. Satu-satunya batasan yang diizinkan ada di aplikasi yang membahayakan jaringan lokal.

Pendukung netralitas jaringan mengakui bahwa keamanan jaringan cukup penting untuk menjamin pengecualian terhadap aturan netralitas jaringan. Mengizinkan penyedia jaringan untuk menyimpang dari netralitas hanya sejauh yang diperlukan untuk melindungi kepercayaan jaringan berakar pada keputusan pengadilan dan peraturan serta aturan administratif yang membantu menetapkan prinsip nondiskriminasi sebagai inti dari netralitas jaringan. Senator Al Franken telah berbicara tentang keputusan FCC "menyebut netralitas bersih 'masalah kebebasan berbicara di zaman kita," Franken (D-MN) menyatakan ketidaksenangannya dengan aturan netralitas bersih FCC baru-baru ini. 'Aturan ini tidak cukup kuat', katanya, menunjukkan bahwa prioritas berbayar tidak dilarang dan jaringan nirkabel diizinkan untuk melakukan diskriminasi sesuka hati. Aturan tersebut menandai 'pertama kalinya FCC mengizinkan diskriminasi di Internet' dan mereka 'pada dasarnya akan menciptakan dua Internet.’

3.6 KUALITAS LAYANAN DAN NETRALITAS BERSIH

Apakah jaringan komunikasi memberikan aplikasi yang Anda harapkan sebagai pelanggan, dengan kecepatan yang dijanjikan dan dengan semua fitur seperti yang diiklankan, bergantung pada kualitas layanan, atau QoS. Konsep ini merupakan bagian dari International Telecommunication Regulations (ITRs), yang menyatakan bahwa administrasi harus ""bekerja sama dalam pembentukan, pengoperasian dan pemeliharaan jaringan internasional untuk memberikan kualitas layanan yang memuaskan," dan bahwa mereka harus "menyediakan dan memelihara, semaksimal mungkin, kualitas layanan minimum." Sejalan dengan perjanjian itu,

ITU telah menerbitkan buku pegangan dan hampir 200 standar teknis (disebut "Rekomendasi") tentang QoS, yang saat ini berlaku. Mereka mencakup parameter seperti:

- kecepatan (throughput data) jaringan akses
- kemacetan di jaringan tulang punggung
- penundaan transmisi (latensi)
- variasi penundaan (jitter), dan
- hilangnya informasi selama transmisi.

Namun, tantangan besar untuk menentukan QoS telah muncul sejak ITR disepakati pada tahun 1988. Telah terjadi pergeseran mendasar dari jaringan tradisional berdasarkan saluran layanan khusus, atau jaringan terpisah untuk setiap layanan. Saat ini, trennya adalah infrastruktur tunggal berdasarkan protokol Internet (IP) untuk memberikan semua layanan, baik suara, video, atau data - dan semakin meningkat hanya ke satu perangkat. Secara tradisional, tanggung jawab untuk QoS dalam komunikasi internasional dibagi di antara jaringan nasional yang mengakhiri. Tetapi dalam jaringan berbasis paket modern, parameter kualitas sebagian besar tidak terdefinisi dan tanggung jawab untuk QoS tidak lagi jelas. Pada dasarnya, dalam lingkungan IP, layanan adalah aplikasi yang dijalankan di peralatan pengguna, dan jaringan itu sendiri tidak dapat sepenuhnya mengontrol kualitas ujung ke ujung dari apa yang dikirimkan. Masalahnya menjadi lebih mendesak dengan peningkatan dramatis dalam komunikasi seluler, yang mungkin mencakup koneksi hybrid dengan jaringan kabel dan terminal. Ditambah lagi, jaringan menjadi semakin padat karena lonjakan lalu lintas data (terutama video). Pendekatan baru diperlukan untuk struktur baru sistem komunikasi saat ini. Untuk terus menyediakan QoS yang memadai, operator jaringan dan penyedia layanan dapat membangun lebih banyak infrastruktur — tetapi ini membutuhkan investasi besar untuk menghadapi pertumbuhan besar yang diharapkan dalam lalu lintas. Solusi paralel adalah manajemen lalu lintas: membuat sistem lebih efisien, sekaligus menetapkan batasan jumlah data yang dapat dikirim, dan siapa yang diprioritaskan sebagai pengirim atau penerima. Bagaimana lalu lintas di jaringan IP dapat — atau apakah seharusnya — dibatasi dengan cara ini terkadang disertakan dalam diskusi tentang "netralitas bersih".

3.7 MODEL HARGA

'Kejahatan diskriminasi harga' selalu disuarakan oleh individu-individu yang dengan sungguh-sungguh mengadvokasi perlunya tarif akses internet universal dan tanpa batas - seringkali sampai-sampai akses internet meteran harus disahkan dari keberadaannya, sehingga dunia digital dapat berkembang tanpa batas dan 'bebas ', seperti yang dimaksudkan oleh penghasutnya. Jika seseorang menggali sedikit lebih dalam, orang mungkin akan menemukan bahwa sebagian besar dari para pendukung yang bersemangat ini saat ini membeli koneksi internet tetap mereka (tanpa tutup) dalam 'bundel triple play' di samping langganan kabel atau IPTV mereka dan beberapa bentuk layanan telepon suara.

Apakah para advokat ini menyadari standar ganda yang mereka tunjukkan ketika menyerukan larangan satu bentuk diskriminasi harga sementara pada saat yang sama mendapat manfaat dari diskriminasi harga yang menopang seluruh kasus bisnis dari pengalaman digital mereka? Karena akses internet 'flat rate' dan paket triple play hanyalah

bentuk lain dari diskriminasi harga. Jika diskriminasi harga adalah ilegal maka tentunya ini juga harus dilarang?

Ambil paket harga flat-rate. Misalkan A dan B sama-sama membeli koneksi internet tarif tetap seharga Rp 450.000 per bulan. Dalam satu bulan, A menggunakan 100 Gb dan B 1 Gb. Penggunaan A lebih mahal daripada penggunaan B, hanya karena menyebabkan lebih banyak kemacetan di jaringan. B membayar Rp 450.000 per Gb untuk lalu lintas yang dipindahkan, tetapi A hanya membayar 30c per Gb. Ini jelas merupakan diskriminasi harga, karena masing-masing membayar harga yang berbeda untuk layanan yang sama. Ini sangat regresif – semakin sedikit sumber daya yang dikonsumsi untuk melayani permintaan, semakin tinggi harga yang harus dibayar. Pengguna bervolume rendah mensubsidi pengguna bervolume tinggi, yang menghasilkan lebih banyak lalu lintas dan berkontribusi pada tingkat kemacetan yang lebih tinggi yang selanjutnya merugikan konsumen bervolume rendah ketika semua harus membayar harga yang lebih tinggi untuk sambungan tarif tetap untuk membiayai pipa yang lebih luas yang harus dipasang ke mengatasi peningkatan volume lalu lintas. Ini bukanlah hasil yang adil – lebih tepatnya, ini adalah 'tragedi milik bersama' di zaman modern. Solusinya, tidak mengherankan, koneksi Internet terukur (juga dikenal sebagai harga berbasis penggunaan) – Sama seperti tol jalan dan biaya berbasis penggunaan lainnya digunakan untuk mengurangi kemacetan dan mendanai rute baru. Sekarang beralih ke bundling. Misalkan pengecer menawarkan sambungan telepon tetap dan sambungan internet yang berdiri sendiri masing-masing seharga Rp 450.000. Misalkan B menghargai penggunaan internet 1 Gb-nya cukup untuk membayar hingga Rp 525.000 per bulan untuk itu, tetapi menghargai sambungan suara saluran tetap hanya Rp 225.000. Di sisi lain, C menghargai suara seharga Rp 525.000 dan potensi penggunaan internet 1 Gb per bulan seharga Rp 300.000. Di bawah harga terpisah, B hanya akan membeli internet seharga Rp 450.000 (meninggalkan surplus Rp 75.000) karena penilaian suaranya (Rp 225.000) lebih rendah dari harga (Rp 450.000). Demikian juga, C hanya akan membeli suara (surplus Rp 75.000) tetapi tidak membeli internet. Misalkan sekarang pengecer menawarkan seikat suara dan internet seharga Rp 735.000, di samping penawaran yang berdiri sendiri. Jika B membeli bundel, keuntungannya adalah Rp 525.000 + Rp 225.000 = Rp 750.000, dikurangi harga Rp 735.000, menyisakan surplus Rp 15.000. Jumlah ini lebih sedikit surplus daripada membeli koneksi internet saja (Rp 75.000), jadi dia tidak membeli paket – dia hanya membeli internet. Dia masih membayar Rp 450.000 per Gb akses internet. Sebaliknya, jika C membeli bundel, keuntungannya adalah Rp 525.000 + Rp 300.000 = Rp 825.000 dikurangi harga yang dibayarkan Rp 735.000, menyisakan surplus Rp 90.000. Ini melebihi surplus dari membeli koneksi suara saja (Rp 75.000), jadi belilah paketnya. Harga marjinal (ekstra) yang dibayarkan untuk internet di atas harga yang dibayarkan untuk suara saja) adalah Rp 285.000. Jadi dia membayar Rp 285.000 per Gb akses internet. Sekali lagi, ini adalah diskriminasi harga – harga yang dibayarkan oleh C untuk layanan yang sama persis seperti yang diterima oleh B lebih rendah. Ergo, bundling memungkinkan terjadinya diskriminasi harga.

Memang, paket bundling telah memungkinkan banyak individu dengan nilai lebih rendah untuk membeli koneksi internet (dan suara dan tv kabel) yang tidak akan pernah dibeli dengan harga yang berdiri sendiri. Pertimbangkan D, yang menghargai 1 Gb internet seharga Rp 375.000 dan suara seharga Rp 375.000. Di bawah harga yang berdiri sendiri, keduanya tidak

akan dibeli, tetapi di bawah bundling, keduanya (surplus Rp 15.000). Operator jaringan selalu menggunakan diskriminasi harga dalam bentuk ini untuk meningkatkan jumlah total sambungan yang terjual, untuk memanfaatkan skala ekonomi yang mengikuti fakta bahwa jaringan memiliki biaya tetap (dan hangus) yang sangat tinggi, tetapi biaya variabel yang rendah. Diskriminasi harga benar-benar standar di semua bentuk transportasi lainnya – seperti warga lanjut usia yang membayar harga diskon untuk perjalanan bus di luar jam sibuk, atau diskon besar untuk tiket multi-perjalanan relatif terhadap harga tiket tunggal – untuk alasan yang persis sama seperti yang digunakan dalam jaringan komunikasi. Seringkali, hal itu dapat membuat perbedaan antara mampu menghasilkan laba komersial pada rute jaringan/bus atau tidak, dan dapat memajukan waktu di mana jaringan tersedia, relatif terhadap penetapan harga yang tidak diskriminatif (dan berdiri sendiri).

Jadi, apakah diskriminasi harga benar-benar 'kejahatan' yang harus dihilangkan jika 'jaring' itu benar-benar 'terbuka'? Jika ya, maka internet akan menjadi sumber daya yang jauh lebih kecil, lebih eksklusif, dan kurang berharga daripada yang muncul sebagai konsekuensi dari serangkaian strategi penetapan harga yang sangat diskriminatif. Kabar baiknya adalah bahwa pengumuman Netralitas Bersih FCC menunjukkan bahwa diskriminasi "baik" (yaitu meningkatkan kesejahteraan) masih mungkin terjadi. Jadi mungkin ada kasus yang sah untuk mengenakan pajak pada distributor konten atas biaya kemacetan yang disebabkan oleh lalu lintas mereka yang bukan konsumen di dunia dengan harga akses internet yang tidak terukur. Memang, ini mungkin hanya perbatasan terakhir untuk 'keadilan' internet untuk semua – dengan cara yang sama seperti mengenakan pajak pada pencemar untuk biaya yang mereka timbulkan terhadap ekonomi atau memungut tol untuk mencegah kemacetan jalan yang mahal.

3.8 NETRALITAS BERSIH DI BAWAH ANCAMAN

Teknik manajemen lalu lintas Internet ("ITM") tertentu saat ini memungkinkan ISP untuk memblokir, menurunkan versi, atau memprioritaskan aliran data tertentu. Penelitian telah menunjukkan bahwa ITM sering digunakan untuk memblokir atau menurunkan lalu lintas Internet tertentu yang berkaitan dengan layanan online yang bersaing dengan layanan lain yang ditawarkan oleh ISP.

Praktik semacam itu membahayakan kapasitas pengguna akhir untuk secara bebas menerima dan menyampaikan informasi secara online menggunakan aplikasi, layanan, dan perangkat pilihan mereka, dan membahayakan karakter arsitektur Internet yang terbuka dan netral. Selain itu, beberapa ISP besar Eropa telah menjelaskan melalui media dan cara lain, seperti rapat pemegang saham dan asosiasi industri, bahwa mereka bermaksud untuk menyimpang dari penyediaan akses Internet yang netral, untuk mendiskriminasi dan memprioritaskan aliran data tertentu dan memonetisasi nilai. bahwa aplikasi, layanan, dan konten online tertentu (dikandung oleh pengguna Internet) disajikan kepada pelanggan mereka. Hal ini menggambarkan bahwa pendekatan-pendekatan Eropa yang ada berdasarkan prinsip-prinsip ekonomi dan hukum persaingan sejauh ini telah gagal untuk sepenuhnya menegakkan prinsip netralitas jaringan, meskipun pasar telekomunikasi Eropa secara umum dianggap relatif kompetitif. Memang, sama seperti hak untuk memilih saja tidak cukup untuk menjamin kebebasan dalam demokrasi konstitusional, kemungkinan untuk beralih penyedia

– yang dapat dilihat sebagai hak untuk 'memilih (ISP) dengan biaya Anda' - tidak cukup untuk cukup menjamin kenikmatan kebebasan pengguna di Internet. Oleh karena itu, tampaknya perlu untuk menanyakan kebijakan dan pendekatan hukum seperti apa yang paling cocok untuk menegakkan prinsip netralitas jaringan dan menjaga nilai layanan publik dari Internet.

3.9 NETRALITAS BERSIH: POSISI AS

Presiden AS Barack Obama mengatakan penyedia layanan Internet harus diatur lebih seperti utilitas publik untuk memastikan mereka memberikan akses yang sama ke semua penyedia konten, memicu protes keras dari perusahaan kabel dan telekomunikasi dan anggota parlemen Republik. Pernyataan rinci Obama tentang masalah "netralitas bersih," sebuah platform dalam kampanye presiden 2008-nya, adalah intervensi yang jarang dilakukan oleh Gedung Putih ke dalam penetapan kebijakan sebuah badan independen. Saham penyedia layanan Internet utama Comcast Corp (CMCSA.O) dan Time Warner Cable Inc (TWC.N) turun tajam setelah Obama mengatakan ISP harus diklasifikasi ulang untuk menghadapi peraturan yang lebih ketat dan dilarang melakukan kesepakatan "jalur cepat" berbayar dengan perusahaan konten. Presiden juga mengatakan aturan baru Komisi Komunikasi Federal harus berlaku sama untuk ISP seluler dan kabel, dengan pengakuan tantangan khusus yang datang dengan mengelola jaringan.

"Sederhananya: Tidak ada layanan yang harus terjebak di 'jalur lambat' karena tidak membayar biaya," kata Obama, saat ini di Asia, dalam sebuah pernyataan yang dikeluarkan oleh Gedung Putih. "Penjagaan gerbang semacam itu akan merusak level playing field yang penting bagi pertumbuhan Internet." Hampir 4 juta komentar membanjiri FCC tahun ini Ketua Tom Wheeler mengusulkan aturan lalu lintas Internet baru pada bulan Mei yang akan melarang ISP memblokir konten apa pun tetapi mengizinkan perusahaan konten untuk melakukan kesepakatan "yang wajar secara komersial" untuk memastikan situs web dan aplikasi mereka dimuat dengan lancar dan cepat. Meskipun Wheeler telah berjanji untuk mengawasi setiap kesepakatan prioritas berbayar yang akan merugikan konsumen, kelompok kepentingan publik khawatir bahwa aturan yang diusulkannya akan menciptakan "jalur cepat" bagi perusahaan yang membayar dan menurunkan orang lain ke "jalur lambat". ISP mengatakan mereka belum dan tidak akan mencapai kesepakatan prioritas berbayar tetapi menolak keras prospek diatur lebih seperti utilitas publik. "Klasifikasi ulang ..., yang untuk pertama kalinya akan menerapkan regulasi utilitas era 1930-an ke Internet, tentu saja akan menjadi pembalikan radikal," kata Verizon Communications Inc (VZ.N) dalam sebuah pernyataan. Verizon pada bulan Januari memenangkan kasus pengadilan federal yang menantang rangkaian aturan netralitas bersih FCC sebelumnya, yang memungkinkan diskriminasi lalu lintas yang "masuk akal secara komersial" tetapi mengindikasikan FCC akan tidak menyetujui kesepakatan bayar-untuk-prioritas.

Pengadilan mendukung otoritas komisi untuk mengatur akses broadband tetapi mengatakan badan tersebut menerapkan aturan yang lebih ketat untuk ISP yang tidak sesuai dengan cara FCC mengklasifikasikannya, yaitu sebagai layanan informasi. Pendukung konsumen telah bertahun-tahun menekan FCC untuk mengklasifikasi ulang broadband sebagai layanan telekomunikasi sebagai cara untuk memiliki lebih banyak otoritas pengawasan, tetapi ISP telah berjanji mereka akan melawan masalah ini di pengadilan.

Verizon pada hari Senin mengatakan langkah "percuma" untuk mengklasifikasi ulang mungkin tidak akan diajukan di pengadilan, sementara AT&T mengatakan akan berpartisipasi dalam tantangan hukum.

'OBAMACARE UNTUK INTERNET': Wheeler, teman Obama dan mantan penggalangan dana besar, pada hari Senin menegaskan kembali bahwa dia juga menentang jalur cepat Internet atau kesepakatan prioritas yang berbahaya tetapi mengatakan bahwa pendekatan termasuk klasifikasi ulang ISP untuk mengaturnya secara lebih ketat menimbulkan pertanyaan hukum substantif.

"Kita harus meluangkan waktu untuk menyelesaikan pekerjaan dengan benar, sekali dan untuk semua, agar berhasil melindungi konsumen dan inovator online," kata Wheeler. Obama dan pejabat Gedung Putih lainnya mengakui bahwa FCC, sebagai lembaga independen, pada akhirnya akan membentuk peraturan tersebut. Tetapi anggota parlemen dari Partai Republik dengan cepat memanfaatkan gangguan Obama, beberapa hari setelah partai mereka memenangkan kendali atas kedua majelis Kongres dalam pemilihan paruh waktu yang sebagian besar dipandang sebagai penolakan terhadap kebijakan presiden.

Netralitas bersih adalah Obamacare untuk Internet," kata Senator Ted Cruz dari Texas. "Ini menempatkan pemerintah yang bertanggung jawab untuk menentukan harga Internet, persyaratan layanan, dan jenis produk dan layanan apa yang dapat diberikan." Meskipun pelobi mengatakan upaya legislatif untuk membatalkan aturan baru akan menghadapi veto Gedung Putih, perusahaan kabel dan nirkabel diharapkan beralih ke sekutu Partai Republik di Kongres untuk pengawasan yang lebih ketat terhadap FCC. sektor Internet negara yang dinamis dan kuat dengan aturan yang ditulis hampir 80 tahun yang lalu untuk layanan telepon biasa," kata Senator John Thune, seorang Republikan yang diperkirakan akan memimpin Komite Perdagangan Senat. Wheeler awalnya mendorong untuk memberlakukan kembali aturan netralitas bersih sebelum akhir tahun. , tetapi para ahli pada hari Senin mengatakan perkembangan terakhir mungkin mendorong proses ke 2015. Saham Time Warner Cable turun sebanyak 7,2 persen, dan ditutup turun hampir 5 persen. persen, sedangkan Comcast turun sebanyak 6,1 persen dan ditutup sendiri 4 persen. Comcast, yang tawarannya untuk membeli Time Warner Cable berada di bawah tinjauan peraturan, sejauh ini merupakan saham yang paling aktif diperdagangkan di pasar AS.

3.10 NETRALITAS BERSIH DAN TRAI

Menyusul pelanggaran Airtel terhadap prinsip Netralitas Net, Rahul Khullar, Ketua TRAI, sementara mengakui bahwa Airtel telah melanggar Netralitas Net, membuat beberapa pernyataan yang mengkhawatirkan kepada Financial Express, dan membuat saya bertanya-tanya tentang maksud mengajukan kasus di hadapan juri yang sudah berprasangka buruk, dan apakah konsultasi tersebut akan berakhir menjadi lelucon untuk membenarkan keputusan yang telah diambil oleh TRAI.

Kepada Financial Express, Khullar berkata:

"" Jika para pemain telekomunikasi berada di bawah seperangkat aturan, bukankah seharusnya para pemain OTT juga dibawa di bawah semacam aturan? Kalau tidak, akan ada lapangan bermain yang tidak rata," katanya.

Menunjukkan bagaimana para pemain OTT dapat dibawa ke bawah regulasi, Khullar mengatakan bahwa mungkin ada norma-norma perizinan bagi mereka juga di mana mereka harus membayar biaya lisensi kepada pemerintah berdasarkan bagi hasil. Opsi lainnya, yang lebih sederhana, adalah bahwa biaya pemutusan dikenakan pada panggilan yang berasal dari layanan sejenis Viber atau Skype.

Sementara Khullar menjelaskan kasus untuk membawa aplikasi OTT (yang menurut operator telekomunikasi, termasuk Jejaring Sosial, Pesan Instan (IM), Aplikasi (Aplikasi), VoIP, Layanan Cloud, Televisi Internet, IPTV, komunikasi Mesin ke Mesin), berdebat tentang level playing field, di mana dia menjelaskan sudut pandang konsumen, atau sudut pandang industri Internet? Jika dia harus mengajukan kasus (seharusnya tidak), bukankah seharusnya dia menyajikan kasus dari ketiga sisi, kepada penonton, sebagai juri yang netral dan tidak memihak? Sebaliknya, sementara dia mengatakan tindakan Airtel melanggar netralitas bersih, dia mengklarifikasi bahwa Airtel tidak ilegal untuk melakukannya, dan menyebutkan perlunya lapangan bermain yang seimbang. Di mana perspektif minat konsumen? Terus terang, satu-satunya level playing field yang dibutuhkan adalah agar Airtel, yang menjalankan Wynk, tidak menggunakan perannya sebagai penyedia layanan akses untuk membuat pesaing seperti Saavn dan Gaana menjadi lebih mahal. Ingatlah bahwa Airtel juga menjalankan Airtel Talk, sebuah layanan VoIP. Akankah VoIP di Skype dibuat lebih mahal daripada di Airtel Talk?

Sementara Khullar menjelaskan kasus untuk membawa aplikasi OTT (yang menurut operator telekomunikasi, termasuk Jejaring Sosial, Pesan Instan (IM), Aplikasi (Aplikasi), VoIP, Layanan Cloud, Televisi Internet, IPTV, komunikasi Mesin ke Mesin), berdebat tentang level playing field, di mana dia menjelaskan sudut pandang konsumen, atau sudut pandang industri Internet? Jika dia harus mengajukan kasus (seharusnya tidak), bukankah seharusnya dia menyajikan kasus dari ketiga sisi, kepada penonton, sebagai juri yang netral dan tidak memihak? Sebaliknya, sementara dia mengatakan tindakan Airtel melanggar netralitas bersih, dia mengklarifikasi bahwa Airtel tidak ilegal untuk melakukannya, dan menyebutkan perlunya lapangan bermain yang seimbang. Di mana perspektif minat konsumen?

Terus terang, satu-satunya level playing field yang dibutuhkan adalah agar Airtel yang menjalankan ynk tidak menggunakan perannya sebagai penyedia layanan akses untuk membuat pesaing seperti Saavn dan Gaana menjadi lebih mahal. Ingatlah bahwa Airtel juga menjalankan Airtel Talk, sebuah layanan VoIP. Akankah VoIP di Skype dibuat lebih mahal daripada di Airtel Talk?

Netralitas sangat penting: TRAI perlu mendekati Netralitas Bersih tanpa prasangka. Tiga prinsip inti netralitas:

1. Semua situs harus sama-sama dapat diakses: ISP dan operator telekomunikasi tidak boleh memblokir situs atau aplikasi tertentu hanya karena mereka tidak membayarnya. Tidak ada gateway yang harus dibuat, untuk memberikan penemuan preferensial ke satu situs di atas yang lain.
2. Semua situs harus dapat diakses dengan kecepatan yang sama (pada tingkat ISP/telco): Ini berarti tidak boleh mempercepat situs tertentu karena kesepakatan bisnis. Lebih penting lagi, itu berarti tidak memperlambat beberapa situs.

3. Biaya akses harus sama untuk semua situs (per Kb/Mb atau sesuai paket data): Ini berarti tidak ada "Peringkat Nol". Di negara-negara seperti India, Netralitas Net lebih tentang biaya akses daripada kecepatan akses: semua jalur lambat.

Penting bagi pertumbuhan Internet di India, dan baik konsumen maupun industri Internet (Indoa Digital, siapa saja?) bahwa netralitas harus mutlak, dan prinsip 'pihak yang menelepon membayar' tetap berlaku untuk Internet juga.

3.11 RINGKASAN

Netralitas bersih merupakan fenomena yang sangat penting dari E-security. Dalam unit ini arti dan ruang lingkup netralitas bersih, argumen untuk netralitas bersih, argumen menentang netralitas bersih, diskriminasi data, kualitas layanan dan netralitas bersih, model harga, netralitas bersih di bawah ancaman, posisi AS pada Net-Netralitas, dan Netralitas Net dan TRAI dibahas panjang lebar untuk memahami konsep dan fitur Net-Netralitas. Ini adalah konsep universal dan berlaku untuk semua negara.

3.12 BEBERAPA BUKU BERGUNA

1. Black Ice: Ancaman Terorisme Cyber yang Tak Terlihat oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
2. Cyber Crime dan Cyber Terrorism oleh R.K. Pradhan (Publikasi Mangalam)
3. Cyber Crime dan Cyber Terrorism oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
4. Terorisme Cyber oleh S. Venkatesh (Penulis)
5. Keamanan Crypto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
6. Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
7. Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
8. Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
9. Buku Pegangan Keamanan, Kriptografi dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
10. Hukum Cyber dan Perlindungan IT oleh Harsh Cander (Publikasi PHI)
11. Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
12. Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
13. Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
14. Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
15. Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
16. Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
17. Ruang Siber dan Keamanan Siber oleh Progressive Management (Publikasi Manajemen Progresif)
18. Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)

19. Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

3.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut yang benar dan salah:

A. Netralitas Net juga dikenal sebagai Netralitas Jaringan, Netralitas Internet atau Kualitas Net.

B. India saat ini tidak memiliki undang-undang tentang Netralitas Bersih.

C. Asosiasi Perpustakaan Amerika adalah pendukung kuat kebebasan intelektual.

D. TRAI perlu mendekati Net-Netralitas tanpa prasangka.

E. Salah satu prinsip inti netralitas adalah "semua situs harus sama-sama dapat diakses".

B. Isi Bagian yang Kosong:

i. Istilah netralitas bersih diciptakan oleh Profesor Hukum Media Universitas Columbia.....

ii. Pengguna dapat mengakses situs web atau layanan web resmi apa pun tanpa campur tangan dari.....

iii. Netralitas Jaringan atau Netralitas Jaringan adalah konsep dari.....

iv. Prinsip dasar diskriminasi data adalah.....

v. ..... teknik saat ini memungkinkan ISP untuk memblokir, menurunkan atau memprioritaskan aliran data tertentu.

3.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Tim Wu pada tahun 2003
2. ISP
3. Non-diskriminasi online
4. Sensor
5. Manajemen Lalu Lintas Internet (ITM) Tertentu

3.15 PERTANYAAN TERMINAL

a. Apa pengertian dan ruang lingkup Net-Netralitas?
b. Apa argumen yang mendukung Net-Netralitas?
c. Apa argumen yang menentang Net-Netralitas?
d. Tentukan diskriminasi data.
e. Apa itu model penetapan harga?

BAB 4
PENGAKUAN HUKUM TANDA TANGAN DIGITAL

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan terkait Pengakuan Hukum Tanda Tangan Digital
- Memahami solusi yang tersedia untuk melawan penggunaan Tanda Tangan Digital secara ilegal
- Memahami masalah teknis dan hukum terkait Pengakuan Hukum Tanda Tangan Digital

4.1 PENDAHULUAN

Manfaat utama kriptografi kunci publik adalah menyediakan metode untuk menggunakan tanda tangan digital. Tanda tangan digital memungkinkan penerima informasi untuk memverifikasi keaslian asal informasi, dan juga memverifikasi bahwa informasi tersebut utuh. Dengan demikian, tanda tangan digital menyediakan otentikasi dan integritas data. Tanda tangan digital juga memberikan non-penolakan, yang berarti mencegah pengirim mengklaim bahwa dia tidak benar-benar mengirim informasi. Fitur-fitur ini sama mendasarnya dengan kriptografi seperti privasi, jika tidak lebih. Tanda tangan digital memiliki tujuan yang sama dengan tanda tangan tulisan tangan. Namun, tanda tangan tulisan tangan mudah dipalsukan. Tanda tangan digital lebih unggul daripada tanda tangan tulisan tangan karena hampir tidak mungkin untuk dipalsukan, ditambah lagi membuktikan isi informasi serta identitas penandatangan.

Visi Rencana eGovernance Nasional (NeGP) Pemerintah India adalah untuk "membuat semua layanan Pemerintah dapat diakses oleh orang biasa di wilayahnya, melalui Outlet Pengiriman Layanan Umum dan memastikan efisiensi, transparansi, dan keandalan layanan tersebut dengan biaya terjangkau untuk mewujudkan kebutuhan dasar rakyat jelata". Tujuan utama dari visi tersebut adalah untuk menyediakan layanan elektronik - G2B dan G2C - di mana-mana. Dengan penerapan National eGovernance Plan (NeGP), semakin banyak Departemen/Line Ministries di India yang mengotomatiskan operasi dan proses bisnis mereka serta membuat penyampaian Layanan mereka secara online. Akibatnya, dokumentasi elektronik perlahan meresapi setiap aspek alur kerja bisnis di Departemen Pemerintah. Namun ketika otorisasi tanda tangan diperlukan pada dokumen, salinan cetak dicetak untuk mendapatkan perutean tanda tangan secara fisik. Pengenalan kembali kertas ke dalam alur kerja meningkatkan biaya Pemerintah, membutuhkan waktu tambahan, dan melarang Departemen/Line Kementerian Pemerintah untuk menyadari manfaat sebenarnya dari alur kerja elektronik sepenuhnya.

Tanda Tangan Digital memberikan solusi yang layak untuk membuat catatan elektronik yang dapat ditegakkan secara hukum, menutup celah untuk sepenuhnya tanpa kertas dengan sepenuhnya menghilangkan kebutuhan untuk mencetak dokumen untuk ditandatangani. Tanda tangan digital memungkinkan penggantian proses persetujuan berbasis kertas yang lambat dan mahal dengan yang cepat, murah, dan sepenuhnya digital. Tujuan tanda tangan digital sama dengan tanda tangan tulisan tangan. Alih-alih menggunakan pena dan kertas,

tanda tangan digital menggunakan kunci digital (kriptografi kunci publik). Seperti metode pena dan kertas, tanda tangan digital menempelkan identitas penandatangan pada dokumen dan mencatat komitmen yang mengikat pada dokumen tersebut. Namun, tidak seperti tanda tangan tulisan tangan, pemalsuan tanda tangan digital dianggap tidak mungkin dilakukan seperti tanda tangan tertulis. Selain itu, tanda tangan digital memastikan bahwa setiap perubahan yang dilakukan pada data yang telah ditandatangani tidak dapat tidak terdeteksi.

4.2 KEDUDUKAN HUKUM TANDA TANGAN DIGITAL

Sesuai dengan bagian 2(1) (f) Undang-Undang Teknologi Informasi, 2000 definisi 'tanda tangan digital adalah "tanda tangan digital" berarti otentikasi catatan elektronik apa pun oleh pelanggan melalui metode atau prosedur elektronik sesuai dengan ketentuan pasal 3."

Bagian 5 Undang-Undang Teknologi Informasi, 2000: Pengakuan hukum atas tanda tangan digital: Jika ada orang awam yang menyatakan bahwa informasi atau hal lain apa pun harus disahkan dengan membubuhkan tanda tangan atau dokumen apa pun harus ditandatangani atau dibubuhi tanda tangan siapa pun, maka, meskipun segala sesuatu yang terkandung dalam undang-undang tersebut, persyaratan tersebut dianggap telah dipenuhi jika informasi atau hal tersebut disahkan dengan tanda tangan digital yang dibubuhkan dengan cara yang ditentukan oleh Pemerintah Pusat.

Penjelasan: Untuk keperluan bagian ini, "ditandatangani", dengan variasi tata bahasa dan ekspresi serumpunnya, dengan mengacu pada seseorang, berarti membubuhkan tanda tangannya atau tanda apa pun pada dokumen apa pun dan ungkapan "tanda tangan" harus ditafsirkan sesuai.

Bagian 3 Undang-Undang Teknologi Informasi, 2000: Otentikasi catatan elektronik:

A. Sesuai dengan ketentuan bagian ini, setiap pelanggan dapat mengotentikasi catatan elektronik dengan membubuhkan tanda tangan digitalnya.
B. Otentikasi arsip elektronik dilakukan dengan menggunakan sistem kriptografi asimetris dan fungsi hash yang menyelubungi dan mengubah arsip elektronik awal menjadi arsip elektronik lain.

Penjelasan: Untuk tujuan sub-bagian ini, "fungsi hash" berarti pemetaan algoritma atau terjemahan dari satu urutan bit ke urutan bit lainnya, umumnya lebih kecil, yang dikenal sebagai "hasil hash" sedemikian rupa sehingga catatan elektronik menghasilkan hasil hash yang sama setiap waktu algoritma dieksekusi dengan catatan elektronik yang sama dengan inputnya sehingga secara komputasi tidak layak-

A. Untuk memperoleh atau merekonstruksi catatan elektronik asli dari hasil hash yang dihasilkan oleh algoritma;
B. Bahwa dua catatan elektronik dapat menghasilkan hasil hash yang sama menggunakan algoritma.

4. Setiap orang dengan menggunakan kunci publik pelanggan dapat memverifikasi catatan elektronik.

5. Kunci privat dan kunci publik adalah unik bagi pelanggan dan merupakan pasangan kunci yang berfungsi.

4.3 PENGAKUAN HUKUM CATATAN ELEKTRONIK

Bagian 4 Undang-Undang Teknologi Informasi, 2000: Pengakuan hukum atas arsip elektronik:

Apabila undang-undang menetapkan bahwa informasi atau hal lainnya harus dalam bentuk tertulis atau diketik atau dicetak, maka, terlepas dari apa pun yang terkandung dalam undang-undang tersebut, persyaratan tersebut akan dianggap telah dipenuhi jika informasi atau hal tersebut-

(a) Diberikan atau disediakan dalam bentuk elektronik; dan

(b) Dapat diakses sehingga dapat digunakan untuk referensi berikutnya.

Bagian 6 Undang-Undang Informasi, 2000: Penggunaan catatan elektronik dan tanda tangan digital di Pemerintah dan lembaganya:

(1) Jika ada undang-undang yang mengatur-

i. pengajuan formulir, permohonan atau dokumen lain apa pun dengan otoritas kantor, badan untuk lembaga yang dimiliki atau dikendalikan oleh Pemerintah yang sesuai dengan cara tertentu;

ii. Penerbitan atau pemberian lisensi apa pun, izin. Sanksi atau persetujuan dengan nama apapun yang disebut dengan cara tertentu;

iii. penerimaan atau pembayaran uang dengan cara tertentu, meskipun ada ketentuan dalam undang-undang lain untuk saat ini yang berlaku, persyaratan tersebut akan dianggap telah dipenuhi jika pengajuan, pengeluaran, hibah, penerimaan atau pembayaran tersebut, sebagai dalam hal ini, dilakukan melalui bentuk elektronik seperti yang mungkin ditentukan oleh Pemerintah yang sesuai.

(2) Pemerintah yang sesuai dapat, untuk tujuan ayat (1), dengan peraturan, menetapkan

a) cara dan format di mana catatan elektronik tersebut akan diajukan, dibuat atau diterbitkan;
b) Cara atau metode pembayaran biaya atau biaya apa pun untuk mengajukan, membuat, atau menerbitkan klausul catatan elektronik apa pun (a).

4.4 AMANKAN CATATAN ELEKTRONIK

11. Atribusi catatan elektronik.-

Catatan elektronik harus diatribusikan kepada pembuatnya,-

a) jika dikirim oleh pembuatnya sendiri;
b) oleh seseorang yang memiliki wewenang untuk bertindak atas nama pembuatnya sehubungan dengan catatan elektronik tersebut; atau
c) oleh sistem informasi yang diprogram oleh atau atas nama originator untuk beroperasi secara otomatis.

12. Pengakuan tanda terima.-

(1) Dalam hal pengirim asal tidak setuju dengan penerima bahwa pengakuan penerimaan catatan elektronik diberikan dalam bentuk tertentu atau dengan cara tertentu, pengakuan dapat diberikan oleh-

a) komunikasi apa pun oleh penerima, otomatis atau lainnya; atau

b) setiap perilaku penerima, cukup untuk menunjukkan kepada pengirim bahwa catatan elektronik telah diterima.

Dalam hal Pengirim Asal telah menetapkan bahwa rekaman elektronik hanya akan mengikat pada saat diterimanya pengakuan atas rekaman elektronik tersebut olehnya, maka, kecuali jika pengakuan telah diterima, rekaman elektronik tersebut dianggap tidak pernah dikirim oleh Pengirim Asal.

Apabila pengirim asal tidak menetapkan bahwa rekaman elektronik hanya akan mengikat pada saat diterimanya pengakuan tersebut, dan pengakuan tersebut belum diterima oleh pengirim asal dalam waktu yang ditentukan atau disepakati atau, jika tidak ada waktu yang ditentukan atau disepakati dalam jangka waktu yang wajar. waktu, maka pengirim dapat memberitahukan kepada penerima yang menyatakan bahwa tidak ada pengakuan yang diterima olehnya dan menentukan waktu yang wajar untuk menerimanya dan jika tidak ada pengakuan yang diterima dalam batas waktu yang disebutkan di atas, ia dapat setelah memberikan pemberitahuan kepada penerima, memperlakukan catatan elektronik sebagai keras itu belum pernah dikirim.

13. Waktu dan tempat pengiriman dan penerimaan catatan elektronik

(1) Kecuali jika disepakati lain antara pengirim dan penerima, pengiriman catatan elektronik terjadi ketika memasuki sumber daya komputer di luar kendali pengirim asal.;

Kecuali disepakati lain antara pengirim dan penerima, waktu penerimaan catatan elektronik akan ditentukan sebagai berikut, yaitu:- penerima telah menetapkan sumber daya komputer untuk tujuan menerima catatan elektronik,- penerimaan terjadi pada saat catatan elektronik memasuki sumber daya komputer yang ditunjuk; atau jika catatan elektronik dibelanjakan ke sumber daya komputer penerima yang bukan sumber daya komputer yang ditunjuk, penerimaan terjadi pada saat catatan elektronik diambil oleh penerima; jika penerima tidak menunjuk sumber daya komputer bersama dengan waktu yang ditentukan, jika ada, penerimaan terjadi ketika catatan elektronik memasuki sumber daya komputer penerima. Kecuali jika disepakati lain antara pengirim dan penerima, catatan elektronik dianggap telah diterima di tempat penerima memiliki tempat usahanya.

Ketentuan-ketentuan ayat (2) berlaku meskipun tempat sumber daya komputer berada mungkin berbeda dari tempat catatan elektronik dianggap telah diterima menurut ayat (3). Untuk tujuan bagian ini.- jika pencetus atau penerima memiliki lebih dari satu tempat usaha, tempat usaha utama adalah tempat usaha; jika pengirim atau penerima tidak memiliki tempat usaha, tempat tinggalnya yang biasa dianggap sebagai tempat usaha; "tempat tinggal biasa", dalam kaitannya dengan badan hukum, berarti tempat di mana ia terdaftar.

14. Mengamankan catatan elektronik.-

Apabila prosedur keamanan telah diterapkan pada arsip elektronik pada suatu titik waktu tertentu, maka arsip tersebut akan dianggap sebagai arsip elektronik yang aman dari titik waktu tersebut hingga waktu verifikasi.

4.5 TANDA TANGAN DIGITAL AMAN

15. Tanda tangan digital yang aman.-

Jika, dengan penerapan prosedur keamanan yang disepakati oleh para pihak yang bersangkutan, dapat diverifikasi bahwa tanda tangan digital, pada saat dibubuhkan, adalah –

(a) Unik untuk pelanggan yang membubuhkannya;
(b) Mampu mengidentifikasi pelanggan tersebut;
(c) dibuat dengan cara atau menggunakan sarana di bawah kendali eksklusif pelanggan dan terkait dengan catatan elektronik yang terkait sedemikian rupa sehingga jika catatan elektronik diubah, tanda tangan digital akan menjadi tidak berlaku, maka tanda tangan digital tersebut akan dianggap sebagai tanda tangan digital yang aman.

4.6 SERTIFIKAT TANDA TANGAN DIGITAL

35. Otoritas sertifikasi untuk menerbitkan Sertifikat Tanda Tangan Digital.–

1) Setiap orang dapat mengajukan permohonan kepada Lembaga Sertifikasi untuk penerbitan Sertifikat Tanda Tangan Digital dalam bentuk yang ditetapkan oleh Pemerintah Pusat.
2) Setiap permohonan tersebut harus disertai dengan biaya yang tidak melebihi dua puluh lima ribu rupee sebagaimana ditentukan oleh Pemerintah Pusat, yang harus dibayarkan kepada Otoritas Sertifikasi:

Dengan ketentuan bahwa sementara meresepkan biaya berdasarkan sub-bagian (2) biaya yang berbeda dapat ditentukan untuk kelas pelamar yang berbeda. Setiap permohonan tersebut harus disertai dengan praktik sertifikasi pernyataan atau di mana tidak ada pernyataan seperti itu, pernyataan yang berisi keterangan-keterangan seperti itu, sebagaimana ditentukan oleh peraturan. Pada penerimaan aplikasi berdasarkan sub-bagian (1), Otoritas Sertifikasi dapat, setelah mempertimbangkan pernyataan praktik sertifikasi atau pernyataan lain berdasarkan sub-bagian (3) dan setelah mengajukan pertanyaan yang dianggap sesuai, memberikan Digital Tanda Tangan Sertifikat atau karena alasan untuk dicatat secara tertulis, menolak permohonan:

Asalkan tidak ada Sertifikat Tanda Tangan Digital yang akan diberikan kecuali jika: Otoritas Sertifikasi puas bahwa pemohon memegang kunci pribadi yang sesuai dengan kunci publik untuk dicantumkan dalam Sertifikat Tanda Tangan Digital; pemohon memegang kunci pribadi, yang mampu membuat tanda tangan digital; kunci publik yang akan dicantumkan dalam sertifikat dapat digunakan untuk memverifikasi tanda tangan digital yang dibubuhkan oleh kunci pribadi yang dipegang oleh pemohon: Dengan ketentuan lebih lanjut bahwa tidak ada aplikasi yang akan ditolak kecuali pemohon telah diberi kesempatan yang wajar untuk menunjukkan alasan terhadap penolakan yang diajukan.

36. Representasi pada saat penerbitan Digital Signature Certificate. -

Otoritas Sertifikasi saat menerbitkan Sertifikat Tanda Tangan Digital harus menyatakan bahwa- itu telah mematuhi ketentuan Undang-undang ini dan aturan dan peraturan yang dibuat di bawahnya; telah menerbitkan Sertifikat Tanda Tangan Digital atau dengan cara lain membuatnya tersedia untuk orang yang mengandalkannya dan pelanggan telah menerimanya; pelanggan memegang kunci pribadi yang sesuai dengan kunci publik, yang tercantum dalam Sertifikat Tanda Tangan Digital; kunci publik dan kunci pribadi subcriber merupakan pasangan kunci yang berfungsi; informasi yang terkandung dalam Sertifikat Tanda Tangan Digital adalah akurat; dan tidak memiliki pengetahuan tentang fakta material6, yang jika telah dimasukkan dalam Sertifikat Tanda Tangan Digital akan berdampak buruk pada keandalan representasi dalam klausa (a) hingga (d).

37. Pembekuan Sertifikat Tanda Tangan Digital. -

(1) Dengan tunduk pada ketentuan ayat (2), Otoritas Sertifikasi yang telah menerbitkan Sertifikat Tanda Tangan Digital dapat menangguhkan Sertifikat Tanda Tangan Digital tersebut.- setelah menerima permintaan untuk itu dari - Pelanggan yang tercantum dalam Sertifikat tanda tangan Digital; atau Setiap orang yang diberi wewenang untuk bertindak atas nama pelanggan tersebut; Jika ada pendapat bahwa Sertifikat Tanda Tangan Digital harus ditangguhkan untuk kepentingan umum.

Sertifikat Tanda Tangan Digital tidak akan ditangguhkan untuk jangka waktu lebih dari lima belas hari kecuali pelanggan telah diberi kesempatan untuk didengar pendapatnya tentang masalah tersebut. Pada penangguhan Sertifikat Tanda Tangan Digital berdasarkan bagian ini, Otoritas Sertifikasi harus mengkomunikasikan hal yang sama kepada pelanggan.'

39. Pencabutan Sertifikat Tanda Tangan Digital. -

(1) Otoritas Sertifikasi dapat mencabut Sertifikat Tanda Tangan Digital yang dikeluarkan olehnya. Jika pelanggan atau orang lain yang diberi wewenang olehnya mengajukan permintaan untuk itu; atau setelah kematian pelanggan; atau pada saat pembubaran perusahaan atau pembubaran perusahaan di mana pelanggan adalah perusahaan atau perusahaan.

Dengan tunduk pada ketentuan ayat (3) dan tanpa mengurangi ketentuan ayat (1), Otoritas Sertifikasi dapat mencabut Sertifikat Tanda Tangan Digital yang telah diterbitkan olehnya sewaktu-waktu, jika berpendapat bahwa -fakta material yang dinyatakan dalam Sertifikat Tanda Tangan Digital adalah palsu atau telah disembunyikan; Persyaratan untuk penerbitan Sertifikat Tanda Tangan Digital tidak dipenuhi; Kunci pribadi dari sistem keamanan Otoritas Sertifikasi dikompromikan dengan cara yang secara material mempengaruhi keandalan Sertifikat Tanda Tangan Digital;

Pelanggan telah dinyatakan pailit atau mati atau di mana pelanggan adalah suatu perusahaan atau perusahaan, yang telah dibubarkan, bubar atau tidak ada lagi. Sertifikat Tanda Tangan Digital tidak dapat dicabut kecuali jika pelanggan telah diberi kesempatan untuk didengar pendapatnya mengenai hal tersebut. Pada pencabutan Sertifikat Tanda Tangan Digital berdasarkan bagian ini, Otoritas Sertifikasi harus mengkomunikasikan hal yang sama kepada pelanggan.

39. Pemberitahuan penangguhan atau pencabutan. -

(1) Apabila Sertifikat Tanda Tangan Digital ditangguhkan atau dicabut berdasarkan bagian 37 atau bagian 38, Otoritas Sertifikasi harus menerbitkan pemberitahuan penangguhan atau pencabutan tersebut, tergantung pada keadaan, dalam penyimpanan yang ditentukan dalam Sertifikat Tanda Tangan Digital untuk publikasi pemberitahuan seperti itu. Dimana satu atau lebih repositori ditentukan, Otoritas Sertifikasi akan menerbitkan pemberitahuan tentang penangguhan atau pencabutan tersebut, seperti yang terjadi, di semua repositori tersebut.

4.7 PERATURAN OTORITAS SERTIFIKASI

17. Pengangkatan Controller dan pejabat lainnya. -

1) Pemerintah Pusat dapat, dengan pemberitahuan dalam Lembaran Negara, menunjuk seorang Pengendali Otoritas Sertifikasi untuk tujuan Undang-undang ini dan dapat,

juga dengan pemberitahuan yang sama atau berikutnya, menunjuk sejumlah Deputi Pengendali dan Asisten Pengendali yang dianggapnya bugar.

2) Pengawas menjalankan fungsinya berdasarkan Undang-undang ini dengan tunduk pada kendali umum dan arahan Pemerintah Pusat.
3) Deputi Pengendali dan Asisten Pengendali harus menjalankan fungsi yang ditugaskan kepadanya oleh Pengendali di bawah pengawasan umum dan kendali Pengendali.
4) Kualifikasi, pengalaman dan syarat dan ketentuan pelayanan Pengendali, Deputi Pengendali, dan Asisten Pengendali harus ditentukan oleh Pemerintah Pusat.
5) Kantor Pusat dan Pejabat Cabang dari petugas Pengendali berada di tempat-tempat yang ditentukan oleh Pemerintah Pusat, dan tempat-tempat tersebut dapat didirikan di tempat-tempat yang dianggap cocok oleh Pemerintah Pusat.
6) Harus ada stempel Kantor Pengawas.

18. Fungsi Kontroler. -

Pengendali dapat melakukan semua atau salah satu fungsi berikut, yaitu:-

a) melakukan pengawasan terhadap kegiatan Otoritas Sertifikasi;
b) sertifikasi kunci publik dari Otoritas Sertifikasi;
c) menetapkan standar yang harus dipertahankan oleh Otoritas Sertifikasi;
d) menetapkan kualifikasi dan pengalaman yang harus dimiliki oleh pegawai dari Otoritas Sertifikasi;
e) menetapkan syarat-syarat yang harus dipenuhi oleh Otoritas Sertifikasi untuk menjalankan bisnisnya;
f) menentukan isi materi tertulis, cetak atau visual dan iklan yang dapat didistribusikan atau digunakan sehubungan dengan Sertifikat Tanda Tangan Digital dan kunci publik;
g) menentukan bentuk dan isi Sertifikat Tanda Tangan Digital dan kuncinya;
h) menentukan bentuk cara di mana akun harus dipelihara oleh Otoritas Sertifikasi;
i) menentukan syarat dan ketentuan yang menjadi subjek penunjukan auditor dan remunerasi yang akan dibayarkan kepada mereka;
j) memfasilitasi pembentukan sistem elektronik oleh Otoritas Sertifikasi baik sendiri atau bersama-sama dengan Otoritas Sertifikasi lainnya dan pengaturan sistem tersebut;
k) menentukan cara di mana Otoritas Sertifikasi akan melakukan transaksi mereka dengan pelanggan;
l) menyelesaikan setiap konflik kepentingan antara Otoritas Sertifikasi dan pelanggan;
m) menetapkan tugas Otoritas Sertifikasi;
n) Memelihara basis data yang berisi catatan pengungkapan dari Otoritas Sertifikasi yang berisi hal-hal tertentu yang dapat ditentukan oleh peraturan yang dapat diakses oleh publik.

21. Lisensi Jaringan Digital Signature Certificates. -

1. Dengan tunduk pada ketentuan ayat (2), setiap orang dapat mengajukan permohonan kepada Pengendali untuk mendapatkan izin penerbitan Sertifikat Tanda Tangan Digital.
2. Tidak ada izin yang akan diterbitkan berdasarkan ayat (1), kecuali pemohon memenuhi persyaratan yang berkaitan dengan kualifikasi, keahlian, tenaga kerja, sumber daya

keuangan dan fasilitas infrastruktur lainnya, yang diperlukan untuk menerbitkan Sertifikat Tanda Tangan Digital sebagaimana ditentukan oleh Pemerintah Pusat.

3. Lisensi yang diberikan berdasarkan bagian ini harus-
    a. berlaku untuk jangka waktu yang ditentukan oleh Pemerintah Pusat;
    b. tidak dapat dipindahtangankan atau diwariskan;
    c. Harus tunduk pada syarat dan ketentuan yang ditentukan oleh peraturan.

4.8 KELAS TANDA TANGAN DIGITAL

Selain empat kelas sertifikat yang diberikan di bawah ini, Otoritas Sertifikasi dapat menerbitkan lebih banyak kelas Sertifikat Kunci Publik, tetapi ini harus didefinisikan secara eksplisit termasuk tujuan penggunaan setiap kelas dan metode verifikasi yang mendasari penerbitan sertifikat. Empat kelas yang disarankan adalah sebagai berikut: -

Sertifikat Kelas 0: Sertifikat ini diterbitkan hanya untuk tujuan demonstrasi/pengujian.

Sertifikat Kelas 1: Sertifikat Kelas 1 akan diterbitkan untuk individu/pelanggan swasta. Sertifikat ini akan mengonfirmasi bahwa nama pengguna (atau alias) dan alamat email merupakan subjek yang tidak ambigu dalam database Otoritas Sertifikasi.

Sertifikat Kelas 2: Sertifikat-sertifikat ini akan diterbitkan untuk digunakan oleh personel bisnis dan perorangan. Sertifikat ini akan mengkonfirmasi bahwa informasi dalam aplikasi yang disediakan oleh pelanggan tidak bertentangan dengan informasi dalam basis data konsumen yang dikenal baik.

Sertifikat Kelas 3: Sertifikat ini akan dikeluarkan untuk individu maupun organisasi. Karena ini adalah sertifikat jaminan tinggi, terutama ditujukan untuk aplikasi e-niaga, sertifikat tersebut akan diterbitkan kepada individu hanya pada penampilan pribadi (fisik) mereka di hadapan Otoritas Sertifikasi.

4.9 TANDA TANGAN DIGITAL VS TANDA TANGAN TULISAN TANGAN

Tanda tangan tulisan tangan yang dipindai dan dilampirkan secara digital dengan dokumen tidak memenuhi syarat sebagai Tanda Tangan Digital. Tanda Tangan Digital adalah kombinasi 0 & 1 yang dibuat menggunakan algoritma kripto. Tanda tangan tinta dapat dengan mudah direplikasi dari satu dokumen ke dokumen lain dengan menyalin gambar secara manual atau elektronik. Tanda Tangan Digital secara kriptografis mengikat identitas elektronik ke dokumen elektronik dan tanda tangan digital tidak dapat disalin ke dokumen lain. Selanjutnya, kontrak kertas sering kali memiliki blok tanda tangan tinta di halaman terakhir, yang memungkinkan halaman sebelumnya diganti setelah kontrak ditandatangani. Tanda tangan digital di sisi lain menghitung hash atau intisari dari dokumen lengkap dan perubahan bahkan satu bit di halaman dokumen sebelumnya akan membuat verifikasi tanda tangan digital gagal. Seperti yang dapat dilihat pada gambar di bawah, Tanda Tangan Digital adalah serangkaian bit yang ditambahkan ke dokumen. Ukuran tanda tangan digital tergantung pada fungsi Hash seperti SHA 1 / SHA2 dll yang digunakan untuk membuat intisari pesan dan kunci penandatanganan. Biasanya beberapa byte.

Perbedaan antara Tanda Tangan Elektronik dan Tanda Tangan Digital: Tanda tangan elektronik berarti otentikasi catatan elektronik oleh pelanggan melalui teknik elektronik. Amandemen UU TI pada tahun 2008 telah memperkenalkan istilah tanda tangan elektronik.

Implikasi dari Amandemen ini adalah bahwa ia telah membantu memperluas cakupan UU TI untuk memasukkan teknik-teknik baru ketika dan ketika teknologi tersedia untuk menandatangani arsip elektronik selain dari Tanda Tangan Digital.

Tinjauan tentang cara kerja Tanda Tangan Digital: Tanda Tangan Digital memerlukan pasangan kunci (pasangan kunci asimetris, angka besar yang terkait secara matematis) yang disebut Kunci Publik dan Pribadi. Sama seperti kunci fisik yang digunakan untuk mengunci dan membuka kunci, dalam kriptografi, fungsi yang setara adalah enkripsi dan dekripsi. Kunci pribadi dirahasiakan dengan pemiliknya biasanya pada media yang aman seperti kartu pintar kripto atau token kripto. Kunci publik dibagikan dengan semua orang. Informasi yang dienkripsi oleh kunci pribadi hanya dapat didekripsi menggunakan kunci publik yang sesuai. Untuk menandatangani dokumen elektronik secara digital, pengirim menggunakan Kunci Pribadinya. Untuk memverifikasi tanda tangan digital, penerima menggunakan Kunci Publik pengirim.

Mari kita pahami bagaimana Tanda Tangan Digital bekerja berdasarkan sebuah contoh. Asumsikan Anda akan mengirim draf kontrak ke pengacara Anda di kota lain. Anda ingin memberikan jaminan kepada pengacara Anda bahwa itu tidak berubah dari apa yang telah Anda kirim dan bahwa itu benar-benar dari Anda.

a) Anda menyalin dan menempelkan kontrak ke dalam catatan email. Dapatkan bentuk dokumen elektronik (misalnya: - file word atau pdf)
b) Menggunakan perangkat lunak khusus, Anda mendapatkan hash pesan (string bit ukuran tetap) dari kontrak.
c) Anda kemudian menggunakan kunci pribadi Anda untuk mengenkripsi hash.
d) Hash terenkripsi menjadi tanda tangan digital Anda dari kontrak dan ditambahkan ke kontrak.

Di ujung lain, pengacara Anda menerima pesan.

a) Untuk memastikan kontraknya utuh dan dari Anda, pengacara Anda membuat hash dari kontrak yang diterima.
b) Pengacara Anda kemudian menggunakan kunci publik Anda untuk mendekripsi Tanda Tangan Digital yang diterima dengan kontrak.
c) Jika hash yang dihasilkan dari Tanda Tangan Digital cocok dengan yang dihasilkan pada Langkah 1, integritas kontrak yang diterima diverifikasi.

4.10 KEKUASAAN UNTUK MEMBUAT PERATURAN OLEH PEMERINTAH PUSAT SEHUBUNGAN DENGAN TANDA TANGAN DIGITAL

Bagian 10 Undang-Undang Teknologi Informasi 2000: Kekuasaan untuk membuat peraturan oleh Pemerintah Pusat sehubungan dengan tanda tangan digital: Pemerintah Pusat dapat, untuk tujuan Undang-undang ini, dengan peraturan, menetapkan-

1) jenis tanda tangan digital;
2) cara dan format tanda tangan digital dibubuhkan;
3) cara atau prosedur yang memudahkan identifikasi orang yang membubuhkan tanda tangan digital;
4) proses dan prosedur pengendalian untuk memastikan integritas, keamanan, dan kerahasiaan catatan atau pembayaran elektronik yang memadai; dan

5) hal-hal lain yang diperlukan untuk memberikan akibat hukum terhadap tanda tangan digital.

4.11 RINGKASAN

Konsep tanda tangan digital kini diterima di seluruh dunia dan dilindungi melalui berbagai ketentuan hukum di tingkat nasional dan internasional. Dalam unit ini konsep kedudukan hukum tanda tangan digital, pengakuan hukum arsip elektronik, arsip elektronik aman, tanda tangan digital aman, sertifikat tanda tangan digital, peraturan otoritas sertifikasi, kelas tanda tangan digital, perbedaan tanda tangan digital dan tanda tangan tulisan tangan, dan kewenangan untuk membuat aturan oleh Pemerintah Pusat terkait tanda tangan digital dibahas panjang lebar untuk memahami konsep terkait yang tergabung dalam berbagai undang-undang yang mengatur tanda tangan digital.

4.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Penulis)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)

- Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

4.13 PERIKSA KEMAJUAN ANDA

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Manfaat utama kriptografi publik adalah menyediakan metode untuk menggunakan tanda tangan digital.
b) Tanda tangan digital memiliki tujuan yang sama dengan tanda tangan tulisan tangan.
c) Pasal 37 Undang-Undang Teknologi Informasi tahun 2000 terkait dengan pembekuan sertifikat tanda tangan digital.
d) Pasal 17 UU IT, 2000 terkait dengan penunjukan Pengendali dan Pejabat lainnya.
e) Ada 6 kelas tanda tangan digital.

B. Isi Bagian yang Kosong:

1) Alih-alih menggunakan pena dan kertas, tanda tangan digital menggunakan.....
2) Definisi 'tanda tangan digital' dimasukkan dalam…….... UU IT, 2000.
3) .....UU IT tahun 2000 terkait dengan pengakuan hukum atas arsip elektronik.
4) ..... UU IT, 2000 terkait dengan Secure Digital Signature.
5) .....UU IT Tahun 2000 terkait dengan Certifying Authority untuk menerbitkan sertifikat tanda tangan digital.

4.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Salah

B.

1. Kunci Digital (Kriptografi Kunci Publik)
2. Bagian 2(1)(f)
3. Bagian 4
4. Bagian 15
5. Bagian 35

4.15 PERTANYAAN TERMINAL

1) Mendiskusikan kedudukan hukum tanda tangan digital.
2) Apa yang dimaksud dengan arsip elektronik dan arsip elektronik yang aman?
3) Apa itu sertifikat tanda tangan digital?
4) Membedakan tanda tangan digital dan tanda tangan tulisan tangan.
5) Apa kewenangan Pemerintah Pusat untuk membuat aturan terkait tanda tangan digital?

BAB 5
PEDOMAN AKSESIBILITAS KONTEN WEB (WCAG)

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami masalah dan pokok bahasan yang terkait dengan Pedoman Aksesibilitas Konten Web
- Memahami pendekatan internasional Pedoman Aksesibilitas Konten Web
- Memahami masalah teknis dan hukum yang terkait dengan Pedoman Aksesibilitas Konten Web

5.1 PENGANTAR

Pedoman Aksesibilitas Konten Web (WCAG) dikembangkan melalui proses W3C bekerja sama dengan individu dan organisasi di seluruh dunia, dengan tujuan untuk membuktikan satu standar bersama untuk aksesibilitas konten web yang memenuhi kebutuhan individu, organisasi, dan pemerintah secara internasional. Dokumen WCAG menjelaskan bagaimana membuat konten web lebih mudah diakses oleh penyandang disabilitas. "Konten" web umumnya mengacu pada informasi di halaman web atau aplikasi web, termasuk:

- informasi alami seperti teks, gambar, dan suara
- kode atau markup yang mendefinisikan struktur, presentasi, dll.
- Aksesibilitas web adalah tentang membuat situs web yang dapat diakses oleh orang-orang dari segala usia dan jenis disabilitas.
- Web yang Dapat Diakses berarti bahwa penyandang disabilitas dapat melihat, memahami, menavigasi, dan berinteraksi dengan Web, dan bahwa mereka dapat berkontribusi ke Web.
- Aksesibilitas juga menguntungkan orang tua dan kegunaan umum situs web.
- Aksesibilitas Web Mengurangi Diskriminasi Disabilitas
- Meningkatkan akses penyandang disabilitas terhadap Informasi

Aksesibilitas juga mempertimbangkan cara masyarakat saat ini menggunakan internet, dan fungsi kehidupan masyarakat yang saat ini online. Membuat Web yang Berkeadilan adalah penting karena memungkinkan orang untuk tetap terhubung dengan komunitas secara luas.

5.2 UNTUK SIAPA WCAG?

WCAG terutama ditujukan untuk:

- Pengembang konten web (penulis halaman, perancang situs, dll.)
- Pengembang alat pembuat web
- Pengembang alat evaluasi aksesibilitas web
- Orang lain yang menginginkan atau membutuhkan standar untuk aksesibilitas web

Sumber daya terkait dimaksudkan untuk memenuhi kebutuhan banyak orang yang berbeda, termasuk pembuat kebijakan, manajer, peneliti, dan lainnya.

WCAG adalah standar teknis, bukan pengantar aksesibilitas.

Empat bidang aksesibilitas

- ❖ Dapat dipahami
- ❖ Dapat dioperasikan
- ❖ Dapat dimengerti
- ❖ Kuat

Duduk di bawah empat area ini adalah 12 pedoman. Pedoman memberikan informasi termasuk contoh lulus dan gagal di bidang desain, konten, dan teknologi.

Dapat dipahami

- Alternatif Teks: Menyediakan Alternatif Teks untuk konten non-teks apa pun.
- Media Berbasis Waktu: Menyediakan Alternatif untuk Media Berbasis Waktu.
- Adaptable: Buat konten yang dapat disajikan dengan cara yang berbeda tanpa kehilangan informasi atau struktur.
- Dapat dibedakan: Memudahkan pengguna untuk melihat dan mendengar konten termasuk memisahkan latar depan dari latar belakang.

Dapat dioperasikan

- Keyboard Dapat Diakses: Membuat semua fungsi tersedia dari keyboard.
- Waktu yang Cukup: Sediakan waktu yang cukup bagi pengguna untuk membaca dan menggunakan konten.
- Kejang: Jangan mendesain konten dengan cara yang diketahui dapat menyebabkan kejang.
- Dapat Dinavigasi: Menyediakan cara untuk membantu pengguna menavigasi, menemukan konten, dan menentukan di mana mereka berada.

Dapat dimengerti

- Readable: Membuat konten teks dapat dibaca dan dimengerti.
- Dapat diprediksi: Membuat halaman Web muncul dan beroperasi dengan cara yang dapat diprediksi.
- Bantuan Masukan: Membantu pengguna menghindari dan memperbaiki kesalahan.
- Kokoh
- Kompatibel: Maksimalkan kompatibilitas dengan agen pengguna saat ini dan yang akan datang, termasuk teknologi bantu.

Aksesibilitas Web adalah sesuatu yang sangat kami sukai di Energetica, sederhananya, Energetica adalah Pakar Aksesibilitas. Ada banyak informasi yang harus dipertimbangkan ketika mengembangkan konten yang dapat diakses, dan kami baru saja mulai muncul ke permukaan. Jika organisasi Anda berpikir untuk mengembangkan konten yang dapat diakses, mengapa tidak menghubungi kami.

Informasi Lebih Lanjut: Sekilas tentang Aksesibilitas Web. Jangan tertipu oleh bagian 'sekilas'. Elemen yang membentuk keberhasilan atau kegagalan aksesibilitas web sangat kompleks, dan terkadang subjektif. Saya tahu saya katakan sebelumnya bahwa tidak ada pendekatan "daftar periksa" yang dapat dengan mudah diterapkan pada aksesibilitas - tidak ada tetapi daftarnya bagus dan mudah dibaca, jadi saya telah menyertakan tautan ke sumber daya yang menyertakan daftar periksa di bawah ini.

5.3 APA ITU WCAG 2.0?

WCAG 2.0 adalah standar teknis yang stabil dan dapat direferensikan. Ini memiliki 12 pedoman yang disusun berdasarkan 4 prinsip: dapat dipahami, dapat dioperasikan, dapat dimengerti, dan kuat. Untuk setiap pedoman, ada kriteria keberhasilan yang dapat diuji, yang berada di tiga tingkat: A, AA, dan AAA.

Materi teknis pendukung WCAG 2.0 meliputi:

- Cara Memenuhi WCAG 2.0: Referensi cepat yang dapat disesuaikan untuk persyaratan Pedoman Aksesibilitas Konten Web 2.0 (kriteria keberhasilan) dan teknik pada dasarnya adalah daftar periksa WCAG 2.0. Kebanyakan orang menggunakan referensi cepat ini sebagai sumber utama untuk bekerja dengan WCAG.
- Teknik untuk WCAG 2.0 memberi Anda detail spesifik tentang cara mengembangkan konten Web yang dapat diakses, seperti contoh kode HTML. Tekniknya "informatif", yaitu, Anda tidak harus menggunakannya. Dasar penentuan kesesuaian terhadap WCAG 2.0 adalah kriteria keberhasilan dari standar WCAG 2.0, bukan tekniknya. Baca lebih lanjut di Teknik di FAQ.
- Memahami WCAG 2.0 memiliki panduan tambahan tentang pembelajaran dan penerapan WCAG 2.0 bagi orang-orang yang ingin memahami pedoman dan kriteria keberhasilan secara lebih mendalam.
- WCAG 2.0 disetujui sebagai standar ISO: ISO/IEC 40500:2012. ISO/IEC 40500 persis sama dengan WCAG 2.0 asli, yang diperkenalkan di atas bersama dengan sumber daya pendukung. Konten ISO/IEC 40500 tersedia secara gratis dari www.w3.org/TR/WCAG20; itu tersedia untuk dibeli dari katalog ISO. Manfaat WCAG 2.0 sebagai standar ISO dirangkum dalam ISO di FAQ. Informasi lebih lanjut tentang W3C dan proses ISO ada di FAQ W3C PAS.

Memahami Empat Prinsip Aksesibilitas:

Lapisan Panduan:

Pedoman: Di bawah setiap prinsip ada daftar pedoman yang membahas prinsip tersebut. Ada total 12 pedoman. Daftar panduan yang praktis dapat ditemukan di daftar isi WCAG 2.0. Salah satu tujuan utama dari pedoman ini adalah untuk memastikan bahwa konten dapat diakses secara langsung oleh sebanyak mungkin orang, dan mampu ditampilkan kembali dalam berbagai bentuk agar sesuai dengan kemampuan sensorik, fisik, dan kognitif orang yang berbeda.

Kriteria Sukses: Di bawah setiap pedoman, ada Kriteria Sukses yang menjelaskan secara spesifik apa yang harus dicapai agar sesuai dengan standar ini. Mereka mirip dengan "pos pemeriksaan" di WCAG 1.0. Setiap Kriteria Sukses ditulis sebagai pernyataan yang akan benar atau salah ketika konten Web tertentu diuji terhadapnya. Kriteria Sukses ditulis untuk netral teknologi.

Semua Kriteria Sukses WCAG 2.0 ditulis sebagai kriteria yang dapat diuji untuk menentukan secara objektif apakah konten memenuhi Kriteria Sukses. Sementara beberapa pengujian dapat diotomatisasi menggunakan program evaluasi perangkat lunak, yang lain memerlukan penguji manusia untuk sebagian atau seluruh pengujian.

Meskipun konten mungkin memenuhi Kriteria Sukses, konten mungkin tidak selalu dapat digunakan oleh orang-orang dengan berbagai disabilitas. Tinjauan profesional yang memanfaatkan heuristik kualitatif yang diakui penting dalam mencapai aksesibilitas untuk beberapa audiens. Selain itu, pengujian kegunaan dianjurkan. Pengujian kegunaan bertujuan untuk menentukan seberapa baik orang dapat menggunakan konten untuk tujuan yang dimaksudkan. Konten harus diuji oleh mereka yang memahami bagaimana orang-orang dengan berbagai jenis disabilitas menggunakan Web. Direkomendasikan agar pengguna penyandang disabilitas disertakan dalam kelompok pengujian saat melakukan pengujian pada manusia.

Setiap Kriteria Keberhasilan untuk pedoman memiliki tautan ke bagian dokumen Cara Bertemu yang menyediakan:

- teknik yang memadai untuk memenuhi Kriteria Sukses,
- teknik konsultasi opsional, dan
- Uraian maksud dari Kriteria Sukses, termasuk manfaat, dan contohnya.

5.4 KOMPONEN PENTING AKSESIBILITAS WEB

Adalah penting bahwa beberapa komponen yang berbeda dari pengembangan Web dan interaksi bekerja sama agar Web dapat diakses oleh penyandang disabilitas. Komponen ini meliputi:

- konten - informasi dalam halaman Web atau aplikasi Web, termasuk:
    - informasi alami seperti teks, gambar, dan suara
    - kode atau markup yang mendefinisikan struktur, presentasi, dll.
- Browser web, pemutar media, dan "agen pengguna" lainnya
    - teknologi bantu, dalam beberapa kasus - pembaca layar, keyboard alternatif, sakelar, perangkat lunak pemindaian, dll.
    - pengetahuan pengguna, pengalaman, dan dalam beberapa kasus, strategi adaptif menggunakan Web
    - pengembang - perancang, pembuat kode, penulis, dll., termasuk pengembang penyandang disabilitas dan pengguna yang menyumbangkan konten
    - authoring tools - perangkat lunak yang membuat situs Web
    - alat evaluasi - Alat evaluasi aksesibilitas web, validator HTML, validator CSS, dll.
    - Pengembang web biasanya menggunakan alat pembuat dan alat evaluasi untuk membuat
    - Isi web.
    - Orang ("pengguna") menggunakan browser Web, pemutar media, teknologi bantu, atau "agen pengguna" lainnya untuk mendapatkan dan berinteraksi dengan konten.

Ada saling ketergantungan yang signifikan antara komponen; yaitu, komponen harus bekerja sama agar Web dapat diakses. Misalnya, untuk teks alternatif pada gambar:

- Spesifikasi teknis alamat teks alternatif (misalnya, HTML mendefinisikan atribut teks alternatif (alt) dari elemen gambar (img))
- Pedoman WAI - WCAG, ATAG, dan UAAG, dijelaskan di bawah ini - menentukan cara menerapkan teks alternatif untuk aksesibilitas di berbagai komponen

- Pengembang memberikan kata-kata teks alternatif yang sesuai
- Alat authoring memungkinkan, memfasilitasi, dan mempromosikan penyediaan teks alternatif di halaman Web
- Alat evaluasi digunakan untuk membantu memeriksa apakah ada teks alternatif
- Agen pengguna menyediakan antarmuka manusia dan mesin ke teks alternatif
- Teknologi bantu menyediakan antarmuka manusia ke teks alternatif dalam berbagai modalitas
- Pengguna mengetahui cara mendapatkan teks alternatif dari agen pengguna dan/atau teknologi bantuan sesuai kebutuhan

Ketika fitur aksesibilitas diimplementasikan secara efektif dalam satu komponen, komponen lain lebih mungkin untuk mengimplementasikannya.

- Ketika browser Web, pemutar media, teknologi bantu, dan agen pengguna lainnya mendukung fitur aksesibilitas, pengguna lebih cenderung memintanya dan pengembang lebih mungkin menerapkannya dalam konten mereka.
- Saat pengembang ingin mengimplementasikan fitur aksesibilitas dalam konten mereka, mereka cenderung menuntut agar alat pembuatnya memudahkan penerapan.
- Saat alat pembuat membuat fitur mudah diterapkan, pengembang lebih cenderung menerapkannya dalam konten mereka.
- Saat fitur aksesibilitas diimplementasikan di sebagian besar konten, pengembang dan pengguna cenderung menuntut agar agen pengguna mendukungnya.

Jika fitur aksesibilitas tidak diimplementasikan dalam satu komponen, ada sedikit motivasi bagi komponen lain untuk mengimplementasikannya ketika tidak menghasilkan pengalaman pengguna yang dapat diakses. Misalnya, pengembang tidak mungkin menerapkan fitur aksesibilitas yang tidak didukung oleh alat pembuat dan sebagian besar browser atau teknologi pendukung tidak menerapkannya secara konsisten.

Jika satu komponen memiliki dukungan aksesibilitas yang buruk, terkadang komponen lain dapat mengimbanginya melalui "penyelesaian" yang membutuhkan lebih banyak usaha dan tidak baik untuk aksesibilitas secara keseluruhan. Sebagai contoh,

- ❖ pengembang dapat melakukan lebih banyak pekerjaan untuk mengimbangi kurangnya dukungan aksesibilitas dalam alat pembuat; misalnya, pengkodean markup secara langsung alih-alih melalui alat
- ❖ pengguna dapat melakukan lebih banyak pekerjaan untuk mengimbangi kurangnya dukungan aksesibilitas di browser, pemutar media, dan teknologi bantu serta kurangnya aksesibilitas konten; misalnya, menggunakan browser yang berbeda atau teknologi bantu untuk mengatasi masalah aksesibilitas yang berbeda

Namun, dalam kebanyakan kasus, solusi tidak diterapkan dan hasilnya masih berupa aksesibilitas yang buruk. Selain itu, terkadang dukungan aksesibilitas yang buruk dalam satu komponen tidak dapat diatasi secara wajar oleh komponen lain dan hasilnya adalah tidak dapat diaksesnya, sehingga tidak memungkinkan bagi beberapa penyandang disabilitas untuk menggunakan situs Web, halaman, atau fitur tertentu.

Pedoman untuk Komponen yang berbeda: Konsorsium World Wide Web (W3C) Web Accessibility Initiative (WAI) mengembangkan pedoman aksesibilitas Web untuk berbagai komponen:

- Panduan Aksesibilitas Alat Penulisan (ATAG) membahas alat pembuat
- Pedoman Aksesibilitas Konten Web (WCAG) membahas konten Web, dan digunakan oleh pengembang, alat pembuat, dan alat evaluasi aksesibilitas
- Panduan Aksesibilitas Agen Pengguna (UAAG) membahas browser Web dan pemutar media, termasuk beberapa aspek teknologi bantu

Pedoman WAI didasarkan pada spesifikasi teknis dasar Web, dan dikembangkan dalam koordinasi dengan:

- Spesifikasi teknis W3C (HTML, XML, CSS, SVG, SMIL, dll.)

5.5 IKHTISAR PANDUAN AKSESIBILITAS AGEN PENGGUNA (UAAG)

Dokumen Panduan Aksesibilitas Agen Pengguna (UAAG) menjelaskan bagaimana membuat agen pengguna dapat diakses oleh penyandang disabilitas, khususnya untuk meningkatkan aksesibilitas ke konten Web. Agen pengguna termasuk browser Web, pemutar media, dan teknologi bantu, yang merupakan perangkat lunak yang digunakan beberapa penyandang disabilitas dalam berinteraksi dengan komputer.

UAAG adalah bagian dari serangkaian pedoman aksesibilitas, termasuk Pedoman Aksesibilitas Konten Web (WCAG WG) dan Pedoman Aksesibilitas Alat Penulisan (ATAG). Komponen Penting Aksesibilitas Web menjelaskan hubungan antara pedoman yang berbeda. UAAG terutama untuk pengembang browser Web, pemutar media, teknologi bantu, dan agen pengguna lainnya. UAAG dan sumber daya pendukung juga dimaksudkan untuk memenuhi kebutuhan banyak audiens yang berbeda, termasuk pembuat kebijakan, manajer, dan lainnya. Sebagai contoh:

- Orang yang ingin memilih agen pengguna yang lebih mudah diakses dapat menggunakan UAAG untuk mengevaluasi agen pengguna
- Orang yang ingin mendorong pengembang agen pengguna yang ada untuk meningkatkan aksesibilitas di versi mendatang dapat merujuk vendor agen pengguna ke UAAG

UAAG 1.0 berisi satu set pos pemeriksaan komprehensif yang mencakup:

- Akses ke semua konten, termasuk konten yang terkait dengan peristiwa yang dipicu oleh mouse atau keyboard
- Kontrol pengguna atas bagaimana konten dirender
- Kontrol pengguna atas antarmuka pengguna, dengan dokumentasi fitur aksesibilitas
- Antarmuka pemrograman standar, untuk memungkinkan interaksi dengan teknologi bantu

Format dokumen teknis: UAAG 1.0, dokumen teknik, dan daftar periksa mengikuti format W3C untuk spesifikasi teknis yang mencakup beberapa bagian di awal: tautan ke berbagai versi, editor, hak cipta, abstrak, dan status dengan tautan ke ralat dan email alamat untuk komentar. Sebagian besar spesifikasi WAI memiliki tautan di bagian atas ke Daftar Isi Panduan Aksesibilitas Agen Pengguna 1.0 telah disetujui pada Desember 2002 dan merupakan versi yang stabil dan dapat dirujuk. UAAG 2.0 sedang dikembangkan untuk membantu membuat

generasi masa depan browser Web lebih mudah diakses, untuk memberikan informasi alternatif berdasarkan teknologi dan platform pengguna, dan untuk menyelaraskan dengan WCAG 2.0 dan ATAG 2.0. WAI mengantisipasi UAAG 2.0 dapat selesai pada tahun 2013. Karena sifat dari proses pengembangan W3C, WAI tidak dapat memastikan kapan versi final UAAG 2.0 akan tersedia. UAAG 1.0 akan tetap menjadi versi terbaru yang disetujui hingga versi 2.0 selesai.

Saat ini UAAG 2.0 adalah draft yang matang dan kami berharap konten utama tidak akan berubah secara signifikan. Kami menyarankan Anda menggunakan UAAG 2.0 draft dalam banyak kasus, memahami bahwa itu mungkin berubah. teknis UAAG dokumen dikembangkan oleh User Agent Accessibility Guidelines Working Group (UAWG), yang merupakan bagian dari World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI). Untuk informasi lebih lanjut tentang kelompok kerja.

5.6 SIAPA YANG MENGEMBANGKAN WCAG?

Dokumen teknis WCAG dikembangkan oleh Web Content Accessibility Guidelines Working Group (WCAG WG), yang merupakan bagian dari World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI). WAI memperbarui Teknik untuk WCAG 2.0 dan Memahami WCAG 2.0 secara berkala. Kami menyambut komentar dan pengajuan teknik baru. Peluang untuk berkontribusi pada WCAG dan pekerjaan WAI lainnya diperkenalkan di Berpartisipasi dalam WAI.

16 September 2014 - Kelompok Kerja telah menerbitkan versi terbaru dari Memahami Teknik WCAG 2.0 dan WCAG 2.0. Kelompok Kerja WCAG akan bertemu tatap muka pada tanggal 26 dan 27 Oktober 2014 di Santa Clara, California. Publikasi: WCAG 2.0 diterbitkan sebagai Rekomendasi W3C 11 Desember 2008. Dokumen ini disertai dengan materi pendukung lainnya (diperbarui 16 September 2014) yang dihasilkan oleh Kelompok Kerja WCAG:

- Pedoman Aksesibilitas Konten Web 2.0
- Cara Bertemu WCAG 2.0
- Memahami WCAG 2.0
- Teknik untuk WCAG 2.0
- Menerapkan WCAG 2.0 pada Teknologi Informasi dan Komunikasi Non-Web (WCAG2ICT)

Pedoman Aksesibilitas Konten Web 2.0 adalah dokumen normatif; selebihnya adalah dokumen pendukung.

Kerja saat ini:

WCAG 2.0

Pedoman:

- Draf Kerja WCAG 2.0 dari editor internal saat ini
- WCAG 2.0 versi publik resmi saat ini - 11 Desember 2008
- Bagaimana cara bertemu WCAG 2.0
- Errata dalam Pedoman Aksesibilitas Konten Web 2.0
- Arsip komentar publik
- Wiki digunakan untuk melacak perubahan yang dibahas dalam telekonferensi

- Kuesioner WCAG digunakan untuk mengumpulkan umpan balik kelompok dalam persiapan diskusi
- Persyaratan untuk WCAG 2.0
- Masalah terbuka dipertahankan dalam database WCAG 2.0 Bugzilla; sedang dimigrasikan ke Pelacak Komentar

Memahami WCAG 2.0:

- Working Draft of Understanding WCAG 2.0 . dari editor internal saat ini
- Versi publik formal terkini dari Understanding WCAG 2.0 -16 September 2014

Teknik untuk WCAG 2.0:

- Draft Teknik Kerja internal saat ini untuk WCAG 2.0
- Teknik versi publik saat ini untuk WCAG 2.0 - 16 September 2014
- Persyaratan untuk Daftar Periksa dan Teknik WCAG 2.0
- Formulir pengajuan teknik
- Teknik yang baru saja dikirimkan

Menerapkan WCAG 2.0 ke Teknologi Informasi dan Komunikasi Non-Web (WCAG2ICT)

- Draf WCAG2ICT editor saat ini
- WCAG2ICT versi publik saat ini - 5 September 2013 Menguji

WCAG 2.0

Gugus Tugas Pengembangan Sampel Uji sebelumnya mengembangkan beberapa tes pendahuluan. Gugus Tugas Metodologi Evaluasi WCAG 2.0 (Eval TF) sedang mengerjakan cara untuk menggunakan tes.

Terjemahan WCAG 2.0

Penerjemahan WCAG 2.0 telah dilakukan untuk meningkatkan kesadaran dan memfasilitasi umpan balik pada draft. Halaman terjemahan WCAG 2.0 mencantumkan terjemahan yang tersedia saat ini.

WCAG 1.0

- Errata dalam Pedoman Aksesibilitas Konten Web 1.0
- Tabel WCAG 1.0 Errata - tidak mewakili konsensus atau komitmen untuk menerbitkan WCAG 1.0 yang direvisi.
- Publikasi:

- Pedoman Aksesibilitas Konten Web (WCAG) 2.0 W3C Rekomendasi, 11 Desember 2008
- Cara Bertemu WCAG 2.0
- Memahami WCAG 2.0
- Teknik untuk WCAG 2.0
- Menerapkan WCAG 2.0 pada Teknologi Informasi dan Komunikasi Non-Web (WCAG2ICT)
- Pedoman Aksesibilitas Konten Web (WCAG) 1.0 Rekomendasi W3C, 5 Mei 1999.
  - Terjemahan WCAG 1.0
  - Kesalahan dalam Pedoman Aksesibilitas Konten eb 1.0
- Teknik untuk WCAG 1.0 suite dari W3C Notes, 20 September 2000
  - Teknik untuk Pedoman Aksesibilitas Konten Web 1.0.
  - Teknik Inti untuk Pedoman Aksesibilitas Konten Web 1.0.
  - Teknik HTML untuk Pedoman Aksesibilitas Konten Web 1.0.

- Teknik CSS untuk Pedoman Aksesibilitas Konten Web 1.0.
- Sejarah perubahan teknik.

Dokumen terkait tidak diterbitkan oleh WCAG WG

- Memulai: Membuat Situs Web Dapat Diakses Termasuk tautan ke Skenario, Kiat Cepat, Kurikulum WCAG, FAQ
- Ikhtisar Dokumen WCAG 2.0

5.7 CAKUPAN WCAG 2.0 UNTUK AKSESIBILITAS SELULER

"Aksesibilitas seluler" umumnya mengacu pada pembuatan situs web dan aplikasi lebih mudah diakses oleh penyandang disabilitas saat mereka menggunakan ponsel. Pekerjaan WAI di area ini mencakup orang-orang yang menggunakan berbagai perangkat untuk berinteraksi dengan web: ponsel, tablet, TV, dan banyak lagi.

Halaman ini merangkum sumber daya yang ada dan yang sedang berkembang terkait dengan aksesibilitas web seluler. Tidak ada pedoman terpisah untuk aksesibilitas seluler — seluler tercakup dalam pedoman aksesibilitas W3C yang ada (khususnya WCAG dan UAAG, yang diperkenalkan di bawah).

Pedoman aksesibilitas WAI membahas aksesibilitas seluler:

- WCAG (Pedoman Aksesibilitas Konten Web) mencakup halaman web dan aplikasi web, termasuk konten yang digunakan pada perangkat seluler. Untuk mempelajari bagaimana WCAG mengatasi masalah serupa seperti Praktik Terbaik Web Seluler dan Praktik Terbaik Aplikasi Web Seluler, lihat Pengalaman Web Bersama.
- UAAG (Pedoman Aksesibilitas Agen Pengguna) mencakup browser web dan 'agen pengguna' lainnya, termasuk browser seluler. Untuk contoh bagaimana browser web yang mengikuti UAAG bermanfaat bagi penyandang disabilitas yang menggunakan Web di perangkat seluler, lihat Contoh Aksesibilitas Seluler dari UAAG.
- ATAG (Authoring Tool Accessibility Guidelines) mencakup perangkat lunak yang digunakan untuk membuat halaman web dan aplikasi, termasuk untuk seluler.
- WAI bekerja untuk meningkatkan teknologi untuk aksesibilitas seluler, termasuk:
- IndieUI (Independent User Interface) adalah cara untuk mengkomunikasikan tindakan pengguna ke aplikasi web, termasuk aplikasi seluler. Ini akan memudahkan aplikasi untuk bekerja dengan berbagai perangkat, termasuk teknologi bantu.
- WAI-ARIA (Accessible Rich Internet Applications) mendefinisikan cara untuk membuat konten web lebih mudah diakses, terutama konten dinamis dan kontrol antarmuka pengguna tingkat lanjut. Ini berlaku untuk aplikasi web dan untuk mengakses situs web dengan perangkat seluler.
- W3C membahas aksesibilitas seluler. WAI memastikan bahwa teknologi inti W3C mendukung aksesibilitas, termasuk yang penting untuk web seluler. Semua pekerjaan W3C ditinjau untuk aksesibilitas oleh Kelompok Kerja Protokol dan Format WAI (PFWG). Pekerjaan W3C di ponsel meliputi:
- Praktik Terbaik Aplikasi Web Seluler, Praktik Terbaik Web Seluler, Pemeriksa OK seluler

- Standar untuk Aplikasi Web di Seluler merangkum teknologi yang dikembangkan di W3C yang meningkatkan kemampuan aplikasi web, dan bagaimana penerapannya secara khusus pada konteks seluler.
- Sebagian besar halaman ini membahas penyandang disabilitas yang menggunakan perangkat seluler. Kami juga memiliki sumber daya terkait yang menangani situasi seperti: proyek pengembangan web ingin membuat situs web dan aplikasi web mereka berfungsi lebih baik untuk semua pengguna seluler (termasuk mereka yang tidak cacat) dan juga berfungsi lebih baik untuk pengguna penyandang cacat yang menggunakan komputer "tradisional".
- Aksesibilitas Konten Web dan Web Seluler: Membuat Situs Web Dapat Diakses Baik untuk Penyandang Disabilitas maupun untuk Perangkat Seluler memperkenalkan tumpang tindih yang signifikan antara membuat situs web dapat diakses untuk perangkat seluler dan untuk penyandang disabilitas. Memberikan gambaran singkat yang berguna untuk kasus bisnis.
- Pengalaman Web Bersama: Hambatan yang Umum bagi Pengguna Perangkat Seluler dan Penyandang Disabilitas memberikan contoh hambatan yang dialami penyandang disabilitas dan orang yang menggunakan perangkat seluler saat berinteraksi dengan konten web. Ini diatur oleh prinsip-prinsip yang dapat dipahami, dapat dioperasikan, dapat dipahami, dan kuat, dan mencakup tautan ke bagian yang relevan dari MWBP (Praktik Terbaik Web Seluler) dan WCAG (Pedoman Aksesibilitas Konten Web).
- Hubungan antara Praktik Terbaik Web Seluler (MWBP) dan Pedoman Aksesibilitas Konten Web (WCAG) memberikan panduan bagi orang-orang yang akrab dengan MWBP dan ingin tahu bagaimana kaitannya dengan WCAG, atau akrab dengan WCAG dan ingin tahu bagaimana kaitannya dengan MWBP.
- Pekerjaan WAI saat ini terkait dengan aksesibilitas seluler meliputi:
- IndieUI (Antarmuka Pengguna Independen) - Lihat Ikhtisar IndieUI untuk pengenalan dan tautan ke spesifikasi yang sedang berlangsung serta Kasus Penggunaan dan Persyaratan.
- WAI-ARIA (Aplikasi Internet Kaya yang Dapat Diakses) - Lihat Ikhtisar WAI-ARIA untuk pengenalan dan tautan ke draf dokumen.
- HTML5 melalui Gugus Tugas Aksesibilitas HTML.
- Teknik WCAG dan panduan lain untuk desainer dan pengembang melalui Gugus Tugas Aksesibilitas Seluler.
- Materi UAAG (Pedoman Aksesibilitas Agen Pengguna): Contoh Aksesibilitas Seluler dari UAAG, dan Bagaimana UAAG Berlaku dalam Konteks Seluler (draf kasar Penerapan UAAG ke Ponsel tersedia).
- Laporan Penelitian Aksesibilitas Seluler berdasarkan Simposium Aksesibilitas Seluler pada Juni 2012.
- Database Dukungan Aksesibilitas yang akan memberikan informasi tentang dukungan aksesibilitas dalam teknologi web, termasuk perangkat seluler dan platform seluler.
- Meninjau Standar untuk Aplikasi Web di Ponsel melalui Kelompok Kerja Protokol dan Format (PFWG).

5.8 MEMAHAMI TEKNIK KRITERIA SUKSES WCAG

Pedoman dan kriteria keberhasilan WCAG 2.0 dirancang untuk dapat diterapkan secara luas pada teknologi web saat ini dan masa depan, termasuk aplikasi dinamis, seluler, televisi digital, dll. Mereka stabil dan tidak berubah.

Panduan khusus untuk penulis dan evaluator dalam memenuhi kriteria keberhasilan WCAG disediakan dalam teknik, yang mencakup contoh kode, sumber daya, dan tes. Dokumen Teknik W3C untuk WCAG 2.0 diperbarui secara berkala, sekitar dua kali per tahun, untuk mencakup lebih banyak praktik terbaik saat ini dan perubahan dalam teknologi dan alat.

Tiga jenis panduan dalam Teknik untuk WCAG 2.0 dijelaskan di bawah ini:

- Teknik yang memadai
- Teknik penasehat
- Kegagalan

Juga dijelaskan di bawah ini:

- Teknik umum dan khusus teknologi - yang mungkin cukup atau sebagai nasihat
- Teknik lain - di luar apa yang ada dalam dokumen yang diterbitkan W3C
- Tes teknik
- Agen pengguna dan dukungan teknologi bantu
- Menggunakan teknik - dengan pertimbangan penting

Teknik bersifat informatif—itu artinya tidak diperlukan. Dasar untuk menentukan kesesuaian dengan WCAG 2.0 adalah kriteria keberhasilan dari standar WCAG 2.0—bukan tekniknya. Teknik yang memadai adalah cara yang dapat diandalkan untuk memenuhi kriteria keberhasilan.

- Dari sudut pandang penulis: Jika Anda menggunakan teknik yang memadai untuk kriteria tertentu dengan benar dan didukung oleh aksesibilitas bagi pengguna Anda, Anda dapat yakin bahwa Anda memenuhi kriteria keberhasilan.
- Dari sudut pandang evaluator: Jika konten web menerapkan teknik yang memadai untuk kriteria tertentu dengan benar dan didukung oleh aksesibilitas bagi pengguna konten, konten tersebut sesuai dengan kriteria keberhasilan tersebut.

Teknik penasehatan adalah cara yang disarankan untuk meningkatkan aksesibilitas. Mereka sering sangat membantu beberapa pengguna, dan mungkin satu-satunya cara agar beberapa pengguna dapat mengakses beberapa jenis konten.

Teknik penasihat tidak ditetapkan sebagai teknik yang memadai karena berbagai alasan seperti:

- mereka mungkin tidak cukup untuk memenuhi persyaratan penuh dari kriteria keberhasilan;
- mereka mungkin didasarkan pada teknologi yang belum stabil;
- mereka mungkin tidak mendukung aksesibilitas dalam banyak kasus (misalnya, teknologi bantu belum bekerja dengannya);
- mereka mungkin tidak dapat diuji;
- dalam beberapa keadaan mereka mungkin tidak dapat diterapkan atau praktis, dan bahkan dapat mengurangi aksesibilitas untuk beberapa pengguna sambil meningkatkannya untuk yang lain;

- mereka mungkin tidak membahas kriteria keberhasilan itu sendiri, dan sebaliknya memberikan manfaat aksesibilitas terkait.

Penulis didorong untuk menerapkan semua teknik yang sesuai untuk memenuhi kebutuhan pengguna yang paling luas.

Kegagalan adalah hal-hal yang menyebabkan hambatan aksesibilitas dan gagal kriteria keberhasilan tertentu. Kegagalan yang terdokumentasi berguna untuk:

- Penulis untuk mengetahui apa yang harus dihindari,
- Evaluator yang digunakan untuk memeriksa apakah konten tidak memenuhi kriteria keberhasilan WCAG.

Konten yang gagal tidak memenuhi kriteria keberhasilan WCAG, kecuali jika versi alternatif disediakan tanpa kegagalan. Teknik umum menggambarkan praktik dasar yang berlaku untuk semua teknologi. Teknik khusus teknologi berlaku untuk teknologi tertentu. Beberapa kriteria keberhasilan tidak memiliki teknik khusus teknologi dan hanya dicakup dengan teknik umum. Oleh karena itu, baik teknik umum maupun teknik khusus teknologi yang relevan harus dipertimbangkan. Publikasi teknik untuk teknologi tertentu tidak berarti bahwa teknologi tersebut dapat digunakan di semua situasi untuk membuat konten yang memenuhi kriteria keberhasilan dan persyaratan kesesuaian WCAG 2.0. Pengembang perlu menyadari keterbatasan teknologi tertentu dan menyediakan konten dengan cara yang dapat diakses oleh penyandang disabilitas.

Selain teknik dalam dokumen Teknik W3C untuk WCAG 2.0, ada cara lain untuk memenuhi kriteria keberhasilan WCAG. Teknik W3C tidak komprehensif dan mungkin tidak mencakup teknologi dan situasi yang lebih baru. Konten web tidak harus menggunakan teknik yang diterbitkan W3C agar sesuai dengan WCAG 2.0. (Lihat juga Teknik yang Informatif di atas.)

Penulis konten dapat mengembangkan teknik yang berbeda. Misalnya, seorang penulis dapat mengembangkan teknik untuk HTML5, WAI-ARIA, atau teknologi baru lainnya. Organisasi lain dapat mengembangkan serangkaian teknik untuk memenuhi kriteria keberhasilan WCAG 2.0. Teknik apa pun bisa cukup jika:

- mereka memenuhi kriteria keberhasilan, dan
- semua persyaratan kesesuaian WCAG 2.0 terpenuhi.
- Teknik Mengirim

Kelompok Kerja WCAG mendorong orang untuk mengirimkan teknik baru sehingga mereka dapat dipertimbangkan untuk dimasukkan dalam pembaruan dokumen Teknik untuk WCAG 2.0. Harap kirimkan teknik untuk dipertimbangkan menggunakan Formulir Pengiriman Teknik.

5.9 BAGAIMANA WCAG 2.0 BERBEDA DARI WCAG 1.0

Secara umum, WCAG 2.0 berlaku secara luas untuk teknologi yang lebih maju; lebih mudah digunakan dan dipahami; dan lebih tepat diuji dengan pengujian otomatis dan evaluasi manusia. Masalah mendasar dari aksesibilitas web adalah sama, meskipun ada beberapa perbedaan dalam pendekatan dan persyaratan antara WCAG 1.0 dan WCAG 2.0. Pedoman Aksesibilitas Konten Web 1.0 diterbitkan pada Mei 1999. WCAG 2.0 diterbitkan pada 11 Desember 2008. W3C WAI merekomendasikan penggunaan WCAG 2.0, bukan WCAG 1.0. Sebagian besar situs web yang sesuai dengan WCAG 1.0 seharusnya tidak memerlukan

perubahan signifikan agar sesuai dengan WCAG 2.0, dan beberapa tidak memerlukan perubahan sama sekali. Bagi mereka yang akrab dengan WCAg 1.0, perlu sedikit waktu untuk mempelajari pendekatan baru tentang bagaimana dokumen WCAG 2.0 memberikan panduan.

5.10 PEDOMAN AKSESIBILITAS ALAT PENULISAN (ATAG)

Authoring Tool Accessibility Guidelines (ATAG) Ikhtisar: Alat authoring adalah perangkat lunak dan layanan yang "penulis" (pengembang web, perancang, penulis, dll.) gunakan untuk menghasilkan konten web (halaman web statis, aplikasi web dinamis, dll.). Contoh alat pembuat tercantum di bawah ini di bawah "Untuk Siapa ATAG".

Dokumen Authoring Tool Accessibility Guidelines (ATAG) menjelaskan cara:

- membuat alat pembuatnya sendiri dapat diakses, sehingga penyandang disabilitas dapat membuat konten web, dan
- membantu penulis membuat konten web yang lebih mudah diakses — khususnya: mengaktifkan, mendukung, dan mempromosikan produksi konten yang sesuai dengan Pedoman Aksesibilitas Konten Web (WCAG).

ATAG adalah bagian dari serangkaian pedoman aksesibilitas, termasuk Pedoman Aksesibilitas Konten Web (WCAG) dan Pedoman Aksesibilitas Agen Pengguna (UAAG). Komponen Penting Aksesibilitas Web menjelaskan hubungan antara pedoman yang berbeda.

ATAG terutama untuk pengembang alat pembuat, termasuk jenis alat pembuat berikut:

- alat pembuat halaman web, misalnya, editor HTML apa yang Anda lihat adalah apa yang Anda dapatkan (WYSIWYG)
- perangkat lunak untuk membuat situs web, misalnya, sistem manajemen konten (CMS), alat kursus, agregator konten
- perangkat lunak yang mengubah teknologi konten web, misalnya, pengolah kata dan aplikasi dokumen kantor lainnya dengan "Simpan sebagai HTML"
- alat pembuat multimedia
- situs web yang memungkinkan pengguna menambahkan konten, seperti blog, wiki, situs berbagi foto, forum online, dan situs jejaring sosial
- jenis alat lain yang tercantum dalam definisi glosarium alat pembuat
- ATAG dan sumber daya pendukung juga dimaksudkan untuk memenuhi kebutuhan banyak audiens yang berbeda, termasuk pembuat kebijakan, manajer, dan lainnya. Sebagai contoh:
- Orang yang ingin memilih alat pembuatan yang dapat diakses dan yang menghasilkan konten yang dapat diakses dapat menggunakan ATAG untuk mengevaluasi alat pembuatan.
- Orang yang ingin mendorong pengembang alat pembuat yang ada untuk meningkatkan aksesibilitas di versi mendatang dapat merujuk vendor alat pembuat ke ATAG.

ATAG 2.0 saat ini merupakan "Rekomendasi Kandidat" W3C. (Tahap ini dijelaskan dalam Bagaimana WAI Mengembangkan Pedoman Aksesibilitas melalui Proses W3C.) Untuk memindahkan ATAG 2.0 ke langkah berikutnya menuju Rekomendasi W3C akhir, WAI

meminta pengiriman umpan balik teknis dari pengembang alat pembuat. Anda dapat membantu dengan dua cara:

1. Terapkan satu atau lebih Kriteria Sukses ATAG Jika Anda membuat atau menyesuaikan alat pembuat (lihat Untuk Siapa ATAG), kirimkan contoh alat pembuat Anda untuk menunjukkan bagaimana alat tersebut memenuhi ATAG2.0. Sementara kesesuaian dengan semua kriteria keberhasilan yang berlaku akan diperlukan saat ATAG menjadi Rekomendasi W3C final, tidak perlu mengklaim kesesuaian dengan semua kriteria keberhasilan ATAG 2.0 untuk tahap ini. Anda dapat memilih mana yang akan diajukan untuk pengujian selama tahap Rekomendasi Kandidat ini untuk memverifikasi penerapan kriteria keberhasilan tertentu.
2. Uji kesesuaian ATAG 2.0: Kami membutuhkan sukarelawan dengan pengalaman pengujian aksesibilitas untuk menggunakan proses uji WAI guna memvalidasi bahwa contoh yang dikirimkan benar-benar memenuhi ATAG.

Dokumen teknis ATAG dikembangkan oleh Authoring Tool Accessibility Guidelines Working Group (AUWG), yang merupakan bagian dari World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI). Untuk informasi lebih lanjut tentang kelompok kerja, lihat halaman AUWG.

5.11 RINGKASAN

Unit ini terkait dengan konten web dan pedoman aksesibilitasnya secara global. Dalam hal ini tidak ada perubahan norma domestik dan internasional secara umum. Konsep ini juga bersifat sangat kompleks dan membutuhkan perhatian penuh dengan keahlian teknis pada topik tersebut. Dalam unit ini konsep untuk siapa WCAG, untuk apa WCAG 2.0, komponen aksesibilitas web, pedoman aksesibilitas agen pengguna, siapa yang mengembangkan WCAG, cakupan WCAG2.0 aksesibilitas seluler, pemahaman berbagai teknik WCAG dan kriteria keberhasilan, bagaimana WCAG2.0 berbeda dari WCAG1.0 dan pedoman aksesibilitas alat otoritas dibahas panjang lebar untuk pemahaman dan aplikasi yang lebih baik.

5.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Penulis)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)

- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

5.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Dokumen WCAg menjelaskan bagaimana membuat konten web lebih mudah diakses oleh penyandang disabilitas.
b) Empat bidang aksesibilitas yang dapat dipahami, dapat dioperasikan, dapat dipahami, dan kuat.
c) WCAG2.0 adalah standar ISO yang disetujui.
d) Dokumen UAAG menjelaskan bagaimana membuat agen pengguna dapat diakses oleh penyandang disabilitas, khususnya untuk meningkatkan aksesibilitas ke konten web.
e) WCAG mencakup halaman web dan aplikasi, termasuk konten yang digunakan pada perangkat seluler.

B. Isi Bagian yang Kosong:

i. WCAG adalah ....., bukan pengantar aksesibilitas.
ii. WCAG2.0 adalah ....., standar teknis yang dapat direferensikan.
iii. WCAG artinya.....
iv. ATAG artinya.....
v. Alat ATAG adalah.....

5.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Standar teknis
2. Stabil
3. Pedoman Aksesibilitas Konten Web
4. Pedoman Aksesibilitas Alat Otoritas
5. Perangkat Lunak dan Layanan

5.15 PERTANYAAN TERMINAL

1. Apa itu WCAG2.0?
2. Siapa yang mengembangkan WCAG?
3. Apa itu Pedoman Aksesibilitas Agen Pengguna?
4. Apa saja komponen penting dari Aksesibilitas Web?
5. Bagaimana WCAG2.0 berbeda dari WCAG1.0?

BAB 6
PERANG CYBER TENTANG PRIVASI DAN PENCURIAN IDENTITAS

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami masalah dan pokok bahasan yang terkait dengan Cyber Warfare tentang Privasi dan Pencurian Identitas
- Memahami solusi yang tersedia untuk melawan Cyber Warfare tentang Privasi dan Pencurian Identitas
- Memahami masalah teknis dan hukum yang terkait dengan Cyber Warfare tentang Privasi dan Pencurian Identitas

6.1 PENGANTAR

Istilah pencurian identitas diciptakan pada tahun 1964; namun, secara harfiah tidak mungkin untuk mencuri identitas — istilah yang kurang ambigu adalah penipuan identitas atau peniruan identitas — istilah yang cenderung kurang mengarah pada penempatan tanggung jawab pada orang yang ditiru dan yang cenderung lebih mengarah pada penempatan tanggung jawab yang tepat pada korban dan pelaku. tipuan. "Menentukan hubungan antara pelanggaran data dan pencurian identitas itu menantang, terutama karena korban pencurian identitas sering tidak tahu bagaimana informasi pribadi mereka diperoleh," dan pencurian identitas tidak selalu dapat dideteksi oleh masing-masing korban, menurut laporan yang dilakukan untuk FTC. . Penipuan identitas sering tetapi tidak selalu merupakan konsekuensi dari pencurian identitas. Seseorang dapat mencuri atau menyalahgunakan informasi pribadi tanpa kemudian melakukan pencurian identitas menggunakan informasi tentang setiap orang, seperti ketika terjadi pelanggaran data besar. Sebuah studi Kantor Akuntabilitas Pemerintah AS menetapkan bahwa "sebagian besar pelanggaran tidak mengakibatkan insiden pencurian identitas yang terdeteksi". Laporan itu juga memperingatkan bahwa "sepenuhnya tidak diketahui". Sebuah studi yang tidak dipublikasikan kemudian oleh Universitas Carnegie Mellon mencatat bahwa "Paling sering, penyebab pencurian identitas tidak diketahui," tetapi melaporkan bahwa orang lain menyimpulkan bahwa "kemungkinan menjadi korban pencurian identitas sebagai akibat dari pelanggaran data adalah . .. sekitar hanya 2%". Baru-baru ini, sebuah asosiasi perusahaan data konsumen mencatat bahwa salah satu pelanggaran data terbesar yang pernah ada, terhitung lebih dari empat juta catatan, hanya menghasilkan sekitar 1.800 kasus pencurian identitas, menurut perusahaan yang sistemnya dilanggar.

Pencurian identitas adalah salah satu kekhawatiran yang berkembang dalam kejahatan dunia maya di India saat ini. Menurut Norton Cybercrime Report 2011, secara global 431 juta orang dewasa mengalami kejahatan dunia maya pada tahun 2011 dan lebih dari 1 juta lebih orang dewasa menjadi korban setiap hari. Sesuai laporan, India dengan cepat muncul sebagai sasaran empuk untuk kejahatan dunia maya terorganisir dengan empat dari lima orang dewasa online telah menjadi korban pencurian identitas pada tahun 2011. Pencurian identitas dapat memiliki implikasi keuangan yang serius. "Kartu Kredit dan Debit dapat diajukan atas

nama orang lain. Pemalsuan pinjaman bank dapat diambil atas nama korban. Bahkan berbagai macam hutang dapat terjadi atas nama korban," kata Ian Craig, Managing Director , CPP India.

6.2 PENCURIAN IDENTITAS: KEJAHATAN YANG BERKEMBANG

Pencurian identitas secara luas dianggap sebagai kejahatan dengan pertumbuhan tercepat di dunia. Pertumbuhan pencurian identitas yang cepat disebabkan oleh berbagai cara di mana cara kita menjalani hidup dan memproses informasi telah diubah. Semua perubahan ini memudahkan orang lain untuk mengakses informasi pengenal pribadi kita dan pada akhirnya melubangi identitas kita. Internet telah membuat transmisi informasi pengenal pribadi kami menjadi cepat dan mudah, dan terkadang kurang aman. Kita dapat mengakses rekening band dan kartu kredit secara online, membayar tagihan secara online, serta berbelanja dan melakukan transaksi kartu kredit secara online. Semua proses ini membuat segalanya lebih cepat dan nyaman, tetapi juga menimbulkan risiko terhadap informasi pribadi kita.

Individu dapat membuat spyware yang diinstal pada komputer kita ketika kita menginstal freeware atau program lain dari internet. Spyware ini dapat mengumpulkan informasi tentang situs apa yang akan kita kunjungi, kata sandi apa yang kita gunakan, dan informasi apa yang kita transmisikan, dan kemudian mengirimkannya ke orang lain. Orang ini kemudian dapat menggunakan informasi pribadi kita sendiri atau menjualnya kepada orang lain. Jenis spyware tertentu yang disebut "Trojan horse" bahkan dapat mengizinkan penemunya mengakses komputer dan hard drive kita dari jarak jauh. Saat kami melakukan transaksi kartu kredit online, pengecer online menyimpan informasi kontak dan kartu kredit kami dalam basis data yang kami anggap aman. Agen pemasaran mengumpulkan informasi tentang kebiasaan pengeluaran serta informasi kontak dan informasi pribadi. Ini disimpan dalam database yang kami anggap aman juga.

Namun, karyawan jahat dari jenis perusahaan ini mungkin memiliki akses ke informasi kami. Mereka mungkin disuap untuk memberikan informasi kami atau mereka bahkan mungkin mengambil informasi ini untuk mereka gunakan sendiri atau menjualnya kepada orang lain. Surat pos juga merupakan ancaman. Perusahaan kartu kredit membanjiri pelanggan dan calon pelanggan dengan kartu kredit yang telah disetujui sebelumnya dan cek kehormatan yang dimaksudkan untuk digunakan sebagai pengganti kartu kredit pelanggan. Jika surat ini tidak dibuka dan dihancurkan (sebaiknya menggunakan penghancur kertas) dengan benar, pencuri identitas dapat mengobrak-abrik sampah Anda dan mengambil kredit Anda untuk digunakan sendiri. Di Amerika Serikat, nomor jaminan sosial juga digunakan sebagai sarana identifikasi pribadi lebih umum daripada di masa lalu. Dan semakin banyak pengidentifikasi berharga ini digunakan, semakin mudah bagi seseorang untuk mendapatkan milik Anda dan menggunakannya untuk dirinya sendiri.

Pencurian identitas atau penipuan identitas (true name fraud) adalah pengambilan identitas korban untuk mendapatkan kredit, kartu kredit dari bank dan pengecer, mencuri uang dari rekening keluar korban, mengajukan pinjaman, membuat rekening dengan perusahaan utilitas, menyewa apartemen, mengajukan pailit atau memperoleh pekerjaan atas nama korban. Peniru itu mencuri ribuan rupiah atas nama korban tanpa disadari korban selama berbulan-bulan bahkan bertahun-tahun. Baru-baru ini penjahat telah menggunakan

identitas korban untuk melakukan kejahatan mulai dari pelanggaran lalu lintas hingga kejahatan berat. Banyak tempat yang memiliki pengetahuan tentang identitas seseorang. – Misalnya: dokter pribadi, akuntan, pengacara, dokter gigi, sekolah, tempat kerja, asuransi kesehatan dan banyak lagi yang memiliki informasi identitas diri. Jika seseorang yang berpikiran kriminal bekerja di kantor (atau hanya berkunjung) memutuskan untuk menggunakan informasi ini untuk mengambil identitas seseorang, dia tidak akan mengetahuinya.

Sangat mudah untuk meniru orang lain jika informasi tentang korban sudah siap. Dalam beberapa kasus, yang diperlukan hanyalah tanggal lahir dan informasi pengenal lainnya seperti alamat dan nomor telepon dan apa pun yang dapat mereka ketahui tentang dia. Dengan informasi ini, dan SIM palsu dengan gambar mereka sendiri, mereka dapat memulai kejahatan. Mereka sering memberikan alamat mereka sendiri, mengaku telah pindah. Pemberi kredit yang lalai karena terburu-buru mengeluarkan kredit tidak memverifikasi informasi atau alamat. Jadi begitu penipu membuka akun pertama, mereka menggunakan akun baru ini bersama dengan pengenal lainnya untuk menambah kredibilitas mereka. Ini memfasilitasi proliferasi penipuan. Sekarang si pencuri sedang dalam perjalanan untuk menjadi kaya dan merusak nama baik dan nama baik orang lain. Anda akan memerlukan laporan untuk membersihkan kekacauan kredit. Segera setelah seseorang mengetahui penipuan, dia harus segera mencatat penipuan di akun, memasang peringatan penipuan di profil kreditnya, dan menghubungi polisi di negara tempat penipuan terjadi. Seseorang mungkin tidak dapat segera menghentikan penipuan. Hal ini sangat kompleks. Tapi ini akan membuatnya mulai. Pencurian Identitas terjadi ketika seseorang secara salah menggunakan identitas orang lain untuk mendapatkan kredit, pinjaman, layanan, bahkan sewa dan hipotek atas namanya. Jenis kejahatan ini biasa terjadi di bidang bisnis bank. Penjamin/penjamin biasanya menyamar untuk tujuan pinjaman. Sertifikat gaji karyawan juga dipersonifikasikan untuk pinjaman. Pencurian Identitas adalah pengalaman yang menakutkan dan luar biasa jika itu terjadi pada siapa saja.

Pencurian identitas- Pencurian identitas terjadi ketika penipu mengakses informasi yang cukup tentang identitas seseorang (seperti nama mereka, tanggal lahir, alamat saat ini atau sebelumnya) untuk melakukan penipuan identitas. Pencurian identitas dapat terjadi baik korban penipuan masih hidup atau sudah meninggal. Jika Anda menjadi korban pencurian identitas, hal itu dapat menyebabkan penipuan yang dapat berdampak langsung pada keuangan pribadi Anda dan juga dapat mempersulit Anda untuk mendapatkan pinjaman, kartu kredit, atau hipotek hingga masalah tersebut diselesaikan.

Penipuan identitas: Penipuan identitas dapat digambarkan sebagai penggunaan identitas yang dicuri ditindak pidana untuk memperoleh barang atau jasa dengan cara penipuan. Penipu dapat menggunakan detail identitas Anda untuk:

- Buka rekening bank.
- Dapatkan kartu kredit, pinjaman dan tunjangan negara.
- Memesan barang atas nama Anda.
- Ambil alih akun Anda yang ada.
- Keluarkan kontrak ponsel.
- Dapatkan dokumen asli seperti paspor dan SIM atas nama Anda.

- Mencuri rincian identitas individu tidak dengan sendirinya merupakan penipuan identitas. Tetapi menggunakan identitas itu untuk salah satu kegiatan di atas tidak.

Sumber seperti Pusat Sumber Daya Pencurian Identitas nirlaba membagi pencurian identitas menjadi lima kategori:

- Pencurian identitas kriminal (berpura-pura sebagai orang lain saat ditangkap karena melakukan kejahatan)
- Pencurian identitas keuangan (menggunakan identitas orang lain untuk mendapatkan kredit, barang dan jasa)
- Kloning identitas (menggunakan informasi orang lain untuk mengasumsikan identitasnya dalam kehidupan sehari-hari)
- Pencurian identitas medis (menggunakan identitas orang lain untuk mendapatkan perawatan medis atau obat-obatan)
- Pencurian identitas anak.

Pencurian identitas dapat digunakan untuk memfasilitasi atau mendanai kejahatan lain termasuk imigrasi ilegal, terorisme, phishing, dan spionase. Ada kasus kloning identitas untuk menyerang sistem pembayaran, termasuk pemrosesan kartu kredit online dan asuransi kesehatan.

6.3 PELANGGARAN PRIVASI

Ini adalah kontur hak privasi. Tentu saja, itu tidak mutlak, dan Pengadilan telah bersusah payah untuk menentukannya dalam banyak kesempatan. Lalu, apa yang membenarkan suatu pelanggaran? Pengadilan secara konsisten menyerukan "kepentingan Negara yang memaksa", yang melampaui "kepentingan umum" sederhana yang dikodekan dalam 19 pembatasan. Berdampingan dengan kepentingan Negara yang memaksa, Pengadilan juga mengharuskan – meskipun tidak pernah secara tegas menjabarkannya – undang-undang yang membatasi untuk disesuaikan secara sempit. Dengan kata lain, pemerintah harus menunjukkan bahwa hukum yang dilanggarnya tidak hanya mencapai kepentingan negara yang memaksa, tetapi melakukannya dengan cara yang membatasi privasi dengan cara yang sesempit mungkin. Jika ada cara lain yang mungkin untuk mencapai tujuan yang sama yang tidak melanggar privasi sejauh yang dilakukan oleh undang-undang yang dilanggar, undang-undang tersebut akan dibatalkan.

Kami melihat ini dalam kasus pengawasan polisi, di mana di Gobind, misalnya, Pengadilan membacakan Peraturan 855 persyaratan tambahan gravitasi, untuk memastikan bahwa itu disesuaikan secara sempit; dan kita melihatnya lebih jelas dalam kasus penyadapan telepon, di mana aturan Pengadilan tidak hanya mensyaratkan spesifikasi orang, nomor dan alamat, tetapi juga mengharuskan Negara untuk menggunakan pengawasan hanya jika metode lain tidak cukup terbuka, dan dengan demikian melakukan, untuk melanggar privasi minimal. Penargetan memang sangat penting: semua kasus surveilans yang telah kami jelajahi tidak hanya melibatkan surveilans yang spesifik dan terarah (memang, S. 5(2) dari Undang-Undang Telegraf hanya membayangkan surveilans yang ditargetkan), tetapi fakta bahwa surveilans adalah ditargetkan dan ditujukan pada individu-individu terhadap siapa ada lebih dari alasan kecurigaan yang masuk akal, telah menjadi alasan utama - hampir dispositif - di

mana Pengadilan telah menemukan pengawasan konstitusional. Oleh karena itu, penargetan tampaknya menjadi aspek integral dari penjahitan sempit.

Kekhawatiran yang sangat sah bahwa menciptakan ruang privat hanya berfungsi untuk membenarkan hubungan dominasi dan penindasan non-Negara di dalam ruang itu – baik secara simbolis, dan sebenarnya (lihat, misalnya, pengecualian pemerkosaan dalam perkawinan yang terkenal dalam hukum pidana India). Ini menganggap – alih-alih memperdebatkan – ide filosofis dasar tentang unit utama masyarakat yang tidak dapat dibagi, salep individu yang diatomisasi yang hidup di "zona" privasi yang tertutup rapat, sebuah asumsi yang telah diserang berulang kali dalam lebih dari lima puluh tahun teori sosial . Saya berharap untuk mengeksplorasi argumen-argumen ini di lain hari, tetapi tujuan dari seri ini terutama bersifat doktrinal, bukan filosofis: untuk melihat pengawasan dalam kerangka doktrin konstitusional yang mapan tanpa mempertanyakan – setidaknya untuk saat ini – landasan normatif dari doktrin itu sendiri.

6.4 PENCURIAN IDENTITAS DI BAWAH HUKUM INDIA

Di bawah Undang-Undang TI, 2000 sebagaimana diubah oleh Undang-Undang Teknologi Informasi (Amandemen), 2008, Bagian 66-C berlaku dan Bagian 419 KUHP India, 1860 berlaku. Korban pencurian identitas dapat mengajukan pengaduan di kantor polisi terdekat di mana kejahatan di atas telah dilakukan atau di mana ia mengetahui tentang kejahatan tersebut. Jika kejahatan terbukti, terdakwa diancam dengan hukuman penjara dengan deskripsi baik untuk jangka waktu yang dapat diperpanjang hingga tiga tahun atau dengan denda yang dapat mencapai satu lakh rupee atau dengan keduanya. Sesuai Bagian 77-B UU IT, 2000 pelanggaran di atas dapat dikenali dan dapat ditebus sementara jika Bagian 419 IPC diterapkan bersama dengan Bagian lain s pelanggaran tersebut dapat dikenali, dapat dijaminkan, dapat ditambah dengan izin dari pengadilan di mana penuntutan pelanggaran tersebut tertunda dan diadili oleh hakim manapun.

Bagian 66C dari Undang-Undang Teknologi Informasi, 2000 (Diamandemen pada tahun 2008) adalah Barangsiapa, dengan curang atau tidak jujur, menggunakan tanda tangan elektronik, kata sandi, atau fitur identifikasi unik lainnya dari orang lain, akan dihukum dengan hukuman penjara baik deskripsi untuk jangka waktu yang dapat diperpanjang hingga tiga tahun dan juga akan dikenakan denda yang dapat mencapai satu lakh rupee.

Bagian 419 dalam The Indian Penal Code, 1860: Hukuman untuk kecurangan dengan identitas.—siapa pun yang menipu dengan identitas akan dihukum dengan hukuman penjara baik deskripsi untuk jangka waktu yang dapat diperpanjang hingga tiga tahun, atau dengan denda, atau dengan keduanya.

Bagian 420 IPC, 1860: Ketika penipu menipu orang untuk mengungkapkan data pribadi yang berharga dalam sifat informasi yang dapat diidentifikasi yang kemudian digunakan untuk menipu uang dari rekening korban.

Bagian 468 IPC, 1860: Ketika penipu melakukan pemalsuan situs web yang bersifat catatan elektronik untuk memikat para korban agar memberikan informasi yang dapat diidentifikasi untuk menipu mereka.

Bagian 471 IPC, 1860: Ketika penipu dengan curang atau tidak jujur menggunakan sebagai asli, situs web palsu tersebut di atas bersifat catatan elektronik.

Bagian 66 UU IT, 2000: Ketika penipu dengan informasi identitas yang dicuri mengatakan login id & password, menghapus atau mengubah informasi atau data di rekening korban di server yang merupakan sumber daya komputer.

Bagian 67 UU IT, 2000: Ketika penipu menggunakan informasi yang dicuri seperti profil, detail pribadi & detail kontak korban untuk membuat & memposting profil cabul atas nama korban di situs jejaring sosial.

6.5 TAHAPAN PENCURIAN IDENTITAS

Ada tiga tahap pencurian identitas. Setiap kasus pencurian identitas dapat mencakup satu atau semua tahapan berikut:

- Akuisisi identitas: Ini melibatkan perolehan identitas melalui pencurian, peretasan, pengalihan atau penyadapan surat atau dengan membeli informasi pengenal di internet.
- Penggunaan identitas: Setelah memperoleh identitas, penipu dapat menggunakan identitas tersebut untuk melakukan kejahatan lain yang mengakibatkan keuntungan finansial baginya seperti penyalahgunaan informasi kartu kredit untuk melakukan pembelian online, membuka rekening baru, menjual identitas kepada orang lain yang melakukan penipuan. Terkadang informasi yang dicuri dapat digunakan untuk melecehkan korban, seperti memposting pornografi atau materi cabul oleh penipu yang menyamar sebagai korban.
- Penemuan pencurian: Banyak kasus penyalahgunaan kartu kredit ditemukan dengan cepat, namun dalam beberapa kasus korban pencurian identitas bahkan mungkin tidak tahu bagaimana atau kapan identitas mereka dicuri dan pencurian mungkin memakan waktu 6 bulan hingga beberapa tahun untuk sampai ke tangan mereka. pemberitahuan korban. Studi mengungkapkan bahwa semakin lama waktu yang dibutuhkan untuk mengungkap pencurian, semakin besar kerugian yang dialami korban.

Apa Cara Umum Melakukan Kejahatan Pencurian Identitas?

Berbagai cara yang lazim dilakukan untuk melakukan tindak pidana pencurian identitas yang memanfaatkan internet atau dunia maya dan lain-lain yang tidak, dikenal dengan cara-cara tradisional. Beberapa cara untuk melakukan tindak pidana pencurian identitas yang tidak tuntas adalah sebagai berikut:

- Pencurian: Mungkin ada pencurian dompet atau tas Anda yang berisi kartu kredit bank, paspor, dokumen identitas lainnya yang berisi informasi pribadi penting Anda.
- Peretasan, akses tidak sah ke sistem, dan pencurian basis data : Penipu sering kali mengkompromikan sistem, mengalihkan informasi secara langsung atau tidak langsung dengan bantuan gadget di jaringan. Peretas mendapatkan akses ke basis data rahasia yang sangat besar, mendekripsinya, dan menyalahgunakannya di tempat lain untuk keuntungan finansial atau melakukan penipuan.
- Phishing: Phishing adalah metode yang paling umum untuk mencuri informasi identitas pribadi. Penipu mengirimkan email penipuan dengan tautan ke situs web palsu yang merupakan replika persis dari situs bank asli yang dirancang untuk menipu pengguna sehingga mereka mengungkapkan informasi pribadi mereka.

- Vishing: Ini adalah tindakan menelepon korban melalui telepon oleh penipu yang menyamar sebagai perwakilan bank dalam upaya untuk menipu pengguna korban agar mengungkapkan informasi pribadi.
- Pharming: Ini adalah teknik yang digunakan oleh penipu dengan menyiapkan server web palsu dan mencegat nama pengguna dan nomor PIN.
- Nigerian 419 Scam: Ini adalah metode paling umum yang masih menipu banyak orang di seluruh dunia di mana penipu mengirim email ke orang-orang yang menyamar sebagai anggota keluarga kaya dari Jutawan Afrika yang meninggal yang berada dalam kesulitan karena pergolakan politik di negaranya. Penipu mencari bantuan Anda untuk mendapatkan sejumlah besar uang di akun Anda dengan komisi uang yang sangat besar kepada Anda untuk layanan Anda menawarkan akun Anda untuk menerima uang. Penipuan ini disebut sebagai penipuan Nigeria 419 (untuk bagian yang relevan dari KUHP Nigeria). Ada kategori lain dari penipuan Nigeria yang serupa di mana korban menerima email yang tidak diminta yang menyatakan bahwa dia telah memenangkan lotre setelah emailnya dipilih dari ribuan email lainnya. Penipuan ini memenuhi syarat sebagai kejahatan identitas karena melibatkan pengumpulan informasi pribadi dan bank dari pengguna Internet yang tidak curiga yang cukup mudah tertipu untuk menanggapi ajakan ini.
- Pencurian oleh karyawan dulu & sekarang: Pelaku juga dapat memperoleh informasi pribadi dengan menyuap karyawan yang memiliki akses ke catatan pribadi, basis data, atau informasi rahasia.
- Skimming: Skimming dapat terjadi ketika penjahat menempelkan gadget skimmer kecil ke ATM yang merekam detail strip magnetik kartu ATM dan kamera merekam nomor identifikasi pribadi yang diajukan oleh pengguna.
- Shoulder Surfing: Penipu juga dapat memperoleh data pribadi Anda tanpa membobol rumah Anda. Di tempat-tempat umum, beberapa orang berkeliaran di sekitar ATM & Bilik Telepon yang melihat Anda memasukkan Nomor PIN rahasia Anda atau hanya melihat-lihat di telepon umum atau hanya dengan menguping jika Anda memberikan informasi kartu kredit Anda melalui telepon.
- Dumpster Diving: Merupakan metode yang digunakan pelaku dengan melewati tempat sampah, tempat sampah atau tempat sampah korban. Mereka memperoleh salinan cek, laporan kartu kredit, laporan bank, kuitansi, dan karbon dan mencari apa pun yang memuat nama, alamat, nomor telepon, dan nomor kartu kredit Anda.

6.6 STUDI KASUS: STUXNET, JUNI 2009

Virus Stuxnet yang merusak fasilitas nuklir Natanz Iran "jauh lebih berbahaya daripada senjata siber yang sekarang bersarang di imajinasi publik," kata pakar keamanan siber Ralph Langer kepada Foreign Policy. Stuxnet, sebuah proyek bersama AS-Israel, dikenal karena dilaporkan menghancurkan sekitar seperlima sentrifugal nuklir Iran dengan menyebabkannya lepas kendali. Tetapi eksploit itu memiliki elemen sebelumnya yang lebih rumit dan "mengubah strategi militer global di abad ke-21," menurut Langer. Serangan awal yang kurang dikenal dirancang untuk secara diam-diam menggambar "setara dengan cetak biru listrik pabrik Natanz, untuk memahami bagaimana komputer mengontrol" sentrifugal yang

digunakan untuk memperkaya uranium, Peter Sanger dari The New York Times melaporkan Juni lalu. Langer menambahkan bahwa worm juga secara halus meningkatkan tekanan pada sentrifugal yang berputar sambil menunjukkan kepada ruang kontrol bahwa semuanya tampak normal dengan memutar ulang nilai sistem perlindungan pabrik saat serangan terjadi. Tujuan dari worm tidak ditujukan untuk menghancurkan sentrifugal, tetapi "mengurangi masa pakai sentrifugal Iran dan membuat sistem kontrol mewah Iran muncul di luar pemahaman mereka," tulis Langer.

Dia mencatat bahwa pengkodean itu "sangat jauh, itu membuat orang bertanya-tanya apakah penciptanya mungkin menggunakan narkoba." (Cacing itu dilaporkan diuji di fasilitas nuklir Dimona Israel.) . Hanya setelah bertahun-tahun penyusupan yang tidak terdeteksi, AS dan Israel melepaskan variasi kedua untuk menyerang sentrifugal itu sendiri dan mereplikasi diri ke semua jenis komputer.

Stuxnet kedua dianggap sebagai tindakan kekuatan dunia maya pertama, tetapi rincian baru mengungkapkan bahwa dampak virus pertama akan jauh lebih besar. Itu karena salah satu aspek paling inovatif dari virus awal adalah bagaimana virus itu dikirim ke Natanz melalui thumb drive pekerja, sehingga memanfaatkan tautan terlemah: manusia. Dari Kebijakan Luar Negeri: Kenyataannya adalah bahwa pada skala global, hampir setiap fasilitas industri atau militer yang menggunakan sistem kontrol industri pada skala tertentu bergantung pada jaringan kontraktornya, banyak di antaranya sangat baik dalam tugas-tugas teknis yang didefinisikan secara sempit, tapi buruk di keamanan cyber. Atau seperti yang dikatakan salah satu arsitek rencana Stuxnet kepada Sanger: "Ternyata selalu ada orang bodoh di sekitar yang tidak terlalu memikirkan thumb drive di tangan mereka." Mengingat bahwa penyerang berikutnya mungkin bukan negara-bangsa, mereka mungkin jauh lebih mungkin menyerang infrastruktur penting sipil. Langer mencatat bahwa sebagian besar pabrik modern beroperasi dengan sistem kontrol industri standar, jadi "jika Anda mendapatkan kontrol dari satu sistem kontrol industri, Anda dapat menyusup ke lusinan atau bahkan ratusan jenis yang sama lebih banyak."

6.7 STUDI KASUS-I

Charu Singh (nama diubah), seorang calon pramugari, terkejut ketika pacarnya putus dengannya. Apa yang memicu perpecahan adalah — seseorang meretas akun Facebook-nya dan mengirim pesan buruk tentang dia. Dia mengajukan kasus di Gurgaon Cyber Crime Cell dan penyelidikan selanjutnya membuktikan bahwa teman sekamarnya adalah pelakunya. Menurut polisi, ini bukan hanya kasus satu kali. Ada lonjakan yang mengkhawatirkan dalam kasus pencurian identitas — mencuri detail pribadi seseorang untuk mengakses sumber daya atau mendapatkan kredit atau manfaat lain atas nama orang itu atau menyalahgunakan detail korban untuk tujuan jahat — di Gurgaon.

Hingga Agustus tahun ini, 70 kasus pencurian identitas telah terdaftar di kota Cyber Crime Cell dibandingkan 40 yang dilaporkan tahun lalu. Dalam sebagian besar kasus, penipu mengakses akun individu di berbagai situs jejaring sosial seperti Facebook, Twitter, dan Orkut dan mengambil foto mereka serta informasi lainnya dan menggunakan hal yang sama untuk membuat SIM palsu, mengajukan permohonan sambungan telepon, membuka rekening bank,

dan membuat Kartu PAN dan kartu kredit. Di era digital saat ini, informasi pribadi Anda seperti nama, tanggal lahir, alamat, nomor telepon, ID email mudah diakses secara online dan offline. Informasi yang tersedia dengan mudah tersebut dapat disalahgunakan oleh para penipu. Dengan informasi bit ini, penipu dapat memperoleh koneksi telepon atau kartu kredit yang berpura-pura menjadi Anda. Seseorang tidak akan mengetahui sampai seseorang mendapat pernyataan dari penyedia layanan. Tapi pada saat itu kerusakan sudah terjadi. Polisi mengakui bahwa dalam banyak kasus, korban tidak datang untuk mengajukan kasus. Dalam beberapa kasus, korban menarik kembali pengaduannya setelah mengetahui bahwa orang yang dekat dengan mereka telah melakukan kejahatan. Inspektur Suresh Singh, penanggung jawab Cyber Crime Cell, mengatakan, "Korban sering menarik pengaduan mereka karena sebagian besar terdakwa adalah orang yang dikenal. Banyak siswa tidak menyadari ketika mereka menggunakan webcam untuk berinteraksi dengan teman-teman mereka yang sering merekam video." Baru-baru ini, seorang siswa mengeluh tentang akun Facebook palsunya lengkap dengan detail pribadinya. Belakangan diketahui tersangka adalah mantan pacarnya. Pada bulan Agustus, Ekta Nath, (nama diubah) seorang mahasiswa teknik, mengajukan kasus setelah video intimnya dengan mantan pacarnya diluncurkan di situs porno. Polisi kemudian menangkap mantan pacarnya karena kejahatan tersebut.

6.8 STUDI KASUS-II

Transaksi saham & komoditas penipuan online: Sekarang suatu hari saham dijual dan dibeli secara online. Ada lonjakan dalam kasus di mana pelapor melaporkan bahwa ada akun saham/komoditas online telah disusupi dan transaksi penipuan telah dilakukan oleh penipu yang tidak dikenal yang mengakibatkan kerugian besar baginya. Dalam transaksi online, klien diberikan akun online dengan id & kata sandi klien yang digunakan untuk melakukan transaksi jual & beli melalui server yang berbasis di kantor pialang. Para penipu yang umumnya ahli software atau para eksekutif (core dealer) di kantor broker mencoba untuk mendapatkan client id & password dari kantor broker itu sendiri, metode hit & trial atau social engineering. Setelah memperoleh ID klien & kata sandi, penipu membuat akses tidak sah ke akun klien dan juga mengakses akun mereka sendiri yang keuntungannya akan ditransfer dari akun klien korban. Penipu mengeksekusi transaksi ke akun klien dengan harga yang tidak realistis dan mencocokkan transaksi ini ke akun mereka sendiri secara bersamaan. Dengan cara ini, ia mengalihkan keuntungan ke akunnya sendiri dan kerugian ke akun klien yang tidak menaruh curiga.

Penipuan Bank Phishing: Phishing adalah penipuan pencurian identitas terbesar di Internet dan umum terjadi di India. Dalam beberapa kasus phishing (pelanggaran yang melibatkan pencurian identitas) baru-baru ini yang dilaporkan di India, MO adalah sama yaitu situs Web Bank target palsu dibuat dan pelanggan bank menerima pesan email yang meminta mereka untuk memperbarui layanan tertentu yang mengklaim bahwa kegagalan untuk melakukannya akan mengakibatkan penangguhan atau penghapusan akun mereka. Email tersebut memberikan tautan ke situs phishing, dalam upaya ilegal untuk mengumpulkan informasi pribadi dan akun

Nigerian 419 Scam atau Penipuan Uang Muka: Ada sejumlah kasus melaporkan di mana pelaku penipuan mengirim email ke id email korban, meminta bantuan korban untuk

mengambil dana yang diblokir dan menawarkan persentase yang sehat dari dana ini sebagai komisi. Korban percaya penipu dalam iming-iming menerima dana besar menyampaikan informasi kartu kreditnya, rincian rekening bank untuk penipu.

Pencemaran nama baik atau posting materi porno atau cabul di situs jejaring sosial: Ada juga kasus di mana korban melaporkan bahwa profil dan informasi pribadi mereka telah dicuri dan profil palsu & vulgar atas namanya mengandung pornografi & cabul materi beserta rincian kontak korban seperti nomor telepon & alamat telah diposting di situs jejaring sosial seperti ORKUT.

6.9 STUDI KASUS-III

Mayoritas bank di India telah bermigrasi ke online dan mobile banking. Sebagian besar transaksi dilakukan melalui kartu pembayaran, kartu debit dan kredit, serta saluran elektronik seperti ATM. Akibatnya, baik bank swasta maupun publik, serta lembaga keuangan di India menjadi semakin rentan terhadap serangan dunia maya yang canggih. Menurut RBI, 8322 kasus penipuan dunia maya dilaporkan pada tahun 2012 sebesar 527 juta INR. Meskipun jumlah kasus yang dilaporkan telah menurun dari 15018 kasus yang dilaporkan pada tahun 2010, jumlah yang terlibat dalam kasus tersebut telah meningkat dari 405 menjadi 527 juta INR pada tahun 2012 menyiratkan bahwa nilai rata-rata per kasus penipuan cyber telah meningkat secara signifikan. Salah satu bentuk paling umum dari serangan dunia maya yang berkaitan dengan bank adalah phishing, penipuan keuangan di mana penipu menggunakan teknik rekayasa sosial dan kode spyware atau malware untuk mencuri informasi keuangan dan pribadi rahasia pelanggan seperti nomor rekening bank, nomor kartu kredit, internet kata sandi perbankan, dll. Rincian ini juga dapat digunakan untuk menyedot uang dari rekening bank pelanggan, kerugian yang pada akhirnya harus ditanggung oleh bank itu sendiri. Serangan phishing yang umum melibatkan pengiriman pesan email ke pelanggan yang berisi logo atau gambar yang menyamar sebagai lembaga keuangan. Email-email ini biasanya berisi tautan web yang merupakan laman web berbahaya yang terlihat persis seperti laman web lembaga keuangan. Mayoritas serangan ini dilakukan untuk keuntungan finansial.

Satu dari empat serangan phishing menggunakan domain .IN dan melibatkan penargetan saldo bank pelanggan. Meskipun serangan ini berasal dari seluruh dunia, Hyderabad menjadi tuan rumah dengan jumlah serangan phishing tertinggi kedua di negara ini. Menariknya, kota-kota berkembang seperti Chandigarh, Bhubaneswar, Surat, Cochin, Jaipur, Vishakhapatnam dan Indore juga mengalami serangan phishing.

Kartu kredit selalu menjadi salah satu target terbesar bagi penjahat cyber; bentuk penipuan kartu kredit yang paling umum melibatkan skimming. Dengan peningkatan pesat dalam penggunaan uang plastik, India menyaksikan gelombang penipuan skimming. Skimming adalah pemalsuan teknologi tinggi yang melibatkan penyalinan informasi pelanggan dan kartu yang disimpan pada strip magnetik kartu kredit, termasuk nomor CVV, dengan menggunakan perangkat elektronik yang dikenal sebagai 'skimmer'. Saat kartu kredit digesek melalui perangkat semacam itu, ia membaca dan menangkap informasi yang tersimpan di kartu kredit. Informasi ini digunakan oleh penipu untuk membuat kartu kloning yang kemudian dapat digunakan untuk melakukan transaksi yang tidak sah dan penipuan. Penipuan skimming sangat sulit dideteksi karena kartu kredit tidak benar-benar dicuri atau dilaporkan. Pelanggan

yang memiliki kartu tersebut mengetahui penipuan hanya ketika transaksi dilakukan menggunakan kartu kloning. Jumlah penipuan kartu kredit meningkat meskipun berbagai tindakan proaktif diambil oleh bank-bank India untuk mengatur sistem pengendalian internal untuk mengurangi penipuan yang berkaitan dengan skimming atau kloning kartu kredit. Sesuai statistik RBI, pada kuartal yang berakhir Desember 2012, ada 1590 kasus kartu kredit yang dilaporkan melibatkan 94,86 juta INR dibandingkan dengan 1327 kasus yang dilaporkan pada kuartal yang berakhir September 2012 yang melibatkan 49,29 juta IDR.

Dua jenis serangan skimming yang paling umum terjadi di lokasi berikut:

- ATM
- PoS (point of sale), baik oleh karyawan yang menggunakan perangkat skimming genggam atau penipu yang menukar perangkat PoS dengan perangkat yang telah dimanipulasi untuk menangkap informasi kartu yang tidak sah. misalnya, menggesek kartu kredit di restoran atau pompa bensin.

Contoh-I: Pada Mei 2012, RBI memperingatkan terhadap email penipuan dari id surat: waspada@rbi.org. Surat-surat itu dikirim oleh entitas yang tidak bermoral yang menawarkan platform keamanan online baru dan meminta pelanggan untuk berbagi informasi. Menurut surat tersebut, platform keamanan online baru ditawarkan untuk mencegah pencurian identitas online di internet banking. Email tersebut selanjutnya meminta penerima untuk mengunduh lampiran dan memperbarui informasi mereka. RBI memperingatkan masyarakat untuk tidak membuka email semacam itu atau mencoba mengunduh lampiran di komputer mereka. (Sumber: The Economic Times)

Contoh-II: Pada bulan April 2012, sekelompok penipu berbasis di Indore yang terlibat dalam phishing rekening pelanggan di seluruh negara dua bank terkemuka di India ditangkap. Geng telah membuka rekening fiktif atas nama mereka di setidaknya dua lusin bank berbeda di kota. Rekening ini digunakan untuk menyedot uang dari pemegang rekening bank-bank ini melalui phishing. Uang itu kemudian ditarik dari rekening fiktif melalui ATM atau cek. Terdakwa telah didakwa berdasarkan pasal 419, 420 IPC dan 66 IT Act. (Sumber: The Times of India)

Contoh-III: Pada Januari 2013, dua penduduk Chandigarh menerima tagihan kartu kredit untuk belanja yang dilakukan di Mumbai dan Hyderabad. Uang itu dipotong dari rekening mereka bahkan sebelum mereka bisa mendekati bank. Orang-orang kehilangan uang dengan melakukan pembayaran di pompa bensin di kota Chandigarh. Hampir 55 kasus skimming telah dilaporkan dari pompa bensin di Chandigarh selama enam bulan terakhir. Dalam kasus ini, penjahat mengkloning kartu dan berbelanja di tempat-tempat yang jauh seperti Mumbai dan Hyderabad. Penipuan itu bernilai jutaan. (Sumber: The Times of India)

Contoh-IV: Pada bulan April 2012, sekelompok penipu ditangkap di Hyderabad karena melakukan skimming dan kloning kartu kredit dan debit menggunakan modus operandi yang rumit meretas alamat IP internasional, hawala internet, dan mata-mata dan pencurian data elektronik. Keributan itu terungkap pada Mei 2011 ketika orang-orang yang mengunjungi dua mal mengeluh bahwa sejumlah besar telah ditarik dari rekening mereka. Geng tersebut berhasil menggelapkan 4 hingga 5 crore INR dari pemegang kartu kredit dan debit yang tidak curiga di seluruh negeri — dari Hyderabad ke Delhi, Kolkata ke Bangalore. Mereka menggunakan 15 mesin skimming point of sale (electronic draft capture), satu mesin skimming data ATM, kamera kubah ATM, penulis magnetik elektronik, printer kartu dan mesin

skimmer pin pad ATM dan bahkan menempatkan kamera mata-mata di ATM yang mengambil PIN pengguna . (Sumber: The Indian Express)

6.10 TIPS UNTUK MENCEGAH PENCURIAN IDENTITAS

- Untuk menjaga dari pencurian identitas, jangan pernah memberikan nomor Jaminan Sosial Anda. Perlakukan itu sebagai informasi rahasia.
- Komit semua sandi ke memori. Jangan pernah menuliskannya atau membawanya bersama Anda.
- Saat menggunakan mesin ATM, pastikan tidak ada orang yang berada di atas Anda dan dapat melihat Anda memasukkan kata sandi.
- Saat berpartisipasi dalam lelang online, cobalah untuk membayar penjual secara langsung dengan kartu kredit sehingga Anda dapat mempermasalahkan tagihan jika barang tidak sampai atau disalahartikan. Jika memungkinkan, hindari membayar dengan cek atau wesel.
- Mengadopsi sikap skeptisisme yang sehat terhadap situs web yang menawarkan hadiah atau hadiah. Kemungkinannya adalah, semua yang telah "dimenangkan" adalah kesempatan untuk membeli sesuatu yang tidak Anda inginkan sejak awal.
- Pilih layanan online komersial yang menawarkan fitur kontrol orang tua.
- Beri tahu anak-anak Anda untuk tidak pernah memberikan alamat mereka, nomor telepon, sandi, nama sekolah, atau informasi pribadi lainnya.
- Pastikan anak-anak Anda tahu untuk tidak pernah setuju untuk bertemu langsung dengan seseorang yang mereka temui secara online tanpa mendiskusikannya dengan Anda. Hanya jika Anda memutuskan bahwa tidak apa-apa untuk bertemu dengan "teman dunia maya" mereka jika mereka ingin bertemu dengan orang ini, dan kemudian pertemuan tersebut harus dilakukan di tempat umum yang dikenal di hadapan orang dewasa yang dapat dipercaya.
- Beri tahu anak Anda untuk tidak pernah menanggapi pesan yang berisi kata-kata buruk, menakutkan, atau hanya tampak aneh.
- Beritahu anak-anak Anda untuk tidak pernah memasuki area yang mengenakan biaya untuk layanan tanpa meminta Anda terlebih dahulu.
- Beritahu anak-anak untuk tidak pernah mengirim foto diri mereka kepada siapa pun tanpa izin Anda.
- Pastikan akses Internet di sekolah anak Anda dipantau oleh orang dewasa.
- Dengan kata lain tips berikut agar tidak menjadi korban penipuan:
    1. Waspada: Ini mungkin nasihat paling penting untuk diberikan kepada individu yang peduli tentang pencurian identitas. Waspadai panggilan telepon atau email yang tidak diminta, terutama yang menanyakan detail seperti kata sandi dan detail akun. Jika Anda menerima komunikasi yang mengaku dari bank atau lembaga keuangan lainnya, selalu periksa apakah itu sah. Jika tidak, Anda harus melaporkan aktivitas mencurigakan apa pun kepada perusahaan atau polisi.
    2. Jangan pernah membagikan informasi rahasia: Data rahasia harus persis seperti itu, rahasia. Simpan informasi, seperti nomor pin, detail rekening bank, dan kata sandi, untuk Anda sendiri. Pastikan Anda memiliki nomor pin dan kata sandi yang

berbeda untuk akun dan layanan yang berbeda. Dengan demikian, Anda akan memastikan bahwa jika salah satu dari ini disusupi, maka dampaknya akan terbatas pada satu akun.

3. Periksa laporan bank Anda: Ini adalah sesuatu yang banyak dari kita lalai untuk dilakukan, tetapi memeriksa laporan bank yang ditakuti dapat membantu Anda menghentikan pencurian identitas sebelum menjadi serius. Periksa dengan seksama untuk setiap transaksi yang mencurigakan dan, jika Anda tidak yakin tentang semua ini, konsultasikan dengan bank Anda.
4. Rusak informasi pribadi: Jangan pernah membuang informasi pribadi dan keuangan tanpa merobek-robeknya terlebih dahulu. Banyak penipu terlibat dalam proses yang dikenal sebagai 'bin raiding' untuk mendapatkan informasi pribadi, yang dapat digunakan untuk mencuri identitas Anda. Anda dapat menghindari kompromi detail Anda dengan merobek-robek dokumen sebelum Anda membuangnya.
5. Simpan dokumen penting dengan aman: Simpan dokumen penting, seperti paspor dan SIM Anda, aman dan terlindungi saat Anda tidak membutuhkannya. Jangan membawa kartu kredit dan memeriksa buku di sekitar Anda kecuali benar-benar diperlukan.

6.11 RINGKASAN

Perang dunia maya tentang privasi dan pencurian identitas adalah masalah yang sangat diperdebatkan di seluruh dunia. Dalam unit ini berbagai studi kasus penting digabungkan untuk pemahaman yang lebih baik dan aplikasi praktis. Dalam unit ini konsep pencurian identitas sebagai kejahatan yang berkembang di seluruh dunia, pelanggaran privasi, pencurian India di bawah Hukum India, tahap pencurian identitas dan konsep lainnya dibahas dengan cara akademis yang tepat untuk menjelaskan dalam bahasa yang mudah dan sederhana. Studi kasus Stuxnet dibahas panjang lebar khususnya untuk memahami posisi asing dalam masalah yang sangat kompleks ini.

6.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Penulis)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)

- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

6.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Istilah pencurian identitas diciptakan pada tahun 1964.
b) Pencurian identitas adalah salah satu kekhawatiran yang berkembang dalam kejahatan dunia maya di India saat ini.
c) Ada tiga tahap pencurian identitas.
d) Skimming dapat terjadi ketika seorang penjahat menyerang gadget skimmer kecil ke ATM.
e) Stuxnet adalah virus yang merusak Fasilitas Nuklir Natanz Iran.

B. Isi Bagian yang Kosong:

i Pencurian identitas atau pemalsuan identitas adalah pengambilan identitas korban untuk....., mencuri uang dari milik korban..... dll.
ii Pencurian identitas terjadi ketika penipu mengakses informasi yang cukup tentang identitas seseorang untuk dilakukan.....
iii ..... Undang-undang Teknologi Informasi, 2000 terkait dengan Pencurian Identitas.
iv .....dari KUHP India, 1860 terkait dengan hukuman Pencurian Identitas.
v .....dari IPC terkait dengan ketika penipu secara curang atau tidak jujur menggunakan sebagai asli, situs web palsu yang bersifat catatan elektronik .

6.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA:

A.

1. Benar
2. Benar
3. Benar

4. Benar
5. Benar

B.

1. Dapatkan Kredit, Akun yang Ada
2. Penipuan Identitas
3. Bagian 66-C
4. Bagian 419
5. Bagian 471

6.15 PERTANYAAN TERMINAL:

1. Apa saja cara umum untuk melakukan kejahatan pencurian identitas?
2. Apa itu pencurian identitas?
3. Diskusikan secara rinci pencurian identitas di bawah hukum India.
4. Diskusikan studi kasus Stuxnet.
5. Diskusikan secara rinci dua studi kasus yang terkait dengan pencurian identitas.

BAB 7
SENSOR PENGATURAN HUKUM INTERNASIONAL

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan Penyensoran Pengaturan Hukum Internasional
- Memahami berbagai norma dan aturan terkait Sensor di Seluruh Dunia
- Memahami masalah teknis dan hukum terkait Sensor

7.1 PENGANTAR

Sensor internet di India dilakukan secara selektif oleh pemerintah federal dan negara bagian. Meskipun tidak ada kebijakan atau strategi pemerintah yang berkelanjutan untuk memblokir akses ke konten Internet dalam skala besar, langkah-langkah untuk menghapus konten yang tidak senonoh atau tidak pantas, atau yang membahayakan ketertiban umum atau keamanan nasional telah menjadi lebih umum dalam beberapa tahun terakhir. Namun, situs web yang diblokir baik oleh pemerintah atau penyedia layanan Internet seringkali dapat diakses melalui server proxy. Internet menyediakan informasi penting dan tidak penting bagi jutaan orang di seluruh dunia. Tetapi jika kita mencari informasi yang sama di Cina dan di Republik Ceko, data yang ditemukan mungkin berbeda, karena penyensoran. Sensor internet adalah kontrol informasi di Internet. Di masa lalu, informasi juga disensor. Ada dan ada penyensoran pers, radio, buku, musik, film dan banyak lainnya. Buku-buku dibakar selama rezim Pinochet di Chili pada tahun 1973, karena termasuk informasi yang tidak sesuai untuk rezim. Di beberapa negara, hampir semuanya disensor, di negara lain hanya sedikit, misalnya hanya hal-hal rasis. Pada sensor Internet, beberapa pemerintah mungkin mengontrol penerbitan artikel yang tidak sesuai untuk mereka, atau menekan halaman web yang tidak mereka sukai. Suatu negara dapat meningkatkan sensor Internet karena peristiwa seperti Musim Semi Arab. Sensor internet sangat spesifik, karena memiliki banyak perbedaan dari media lain, ini adalah media yang terdesentralisasi. Ini interaktif, sehingga pembaca dapat menulis komentar, misalnya. Hampir tidak ada batas negara di Internet dan kita dapat membaca informasi dari negara yang sangat jauh. Siapa yang berhak menyensor Internet? Apa yang harus disensor? Selain itu, hubungan hukum antara sensor, pemilik website, pengguna dan penyedia koneksi internet sangat rumit.

7.2 SENSOR INTERNET

Laporan Freedom on the Net 2012: A Global Assessment of Internet and Digital Media yang baru-baru ini diterbitkan oleh Freedom House, sebuah organisasi pengawas independen, menyoroti tren peningkatan penyensoran web di seluruh dunia. Dari 47 negara yang disurvei, ditemukan bahwa sebanyak 19 negara sejak 2011 mengadopsi kebijakan untuk menyensor web, yang secara efektif menghambat pidato online. Sementara negara itu menemukan Estonia dengan tingkat kebebasan Internet terbesar, negara-negara seperti Iran, Kuba, dan Cina ternyata berada di ekstrem yang lain. Pemerintah di banyak negara memainkan skrip

Orwellian dengan memperkenalkan undang-undang kejam untuk menyensor web. Mari kita lihat penyensoran internet yang diikuti di beberapa negara yang menarik banyak perhatian pada tahun lalu.

Sejak beberapa tahun terakhir, kasus sensor internet di India telah meningkat berlipat ganda. pada tahun 2011, India mengadopsi 'Aturan IT 2011' baru yang melengkapi UU IT 2000. Aturan ini mewajibkan perantara Internet untuk menghapus konten yang tidak pantas dalam waktu 36 jam setelah menerima keluhan. Tetapi istilah-istilah yang disertakan tidak jelas dan terbuka untuk interpretasi. Aturan-aturan ini menerima kritik tajam, tetapi mereka telah menang. Pada tahun 2011, pemerintah juga mendapat kritik karena meminta situs-situs besar seperti Google, Facebook, dan Yahoo untuk 'menyaring sebelumnya' konten dan menghapus konten yang tidak pantas dan memfitnah agar tidak ditayangkan. Diduga bahwa pemerintah mendesak perusahaan Internet untuk menggunakan manusia dan bukan mesin untuk melakukan yang diperlukan.

Kemudian pada tahun 2012, perusahaan-perusahaan ini diseret ke pengadilan atas hal yang sama. Perusahaan Internet di pihak mereka berdiri teguh dan menolak untuk mematuhi persyaratan ini. Namun, Laporan Transparansi Google menunjukkan peningkatan permintaan dari pemerintah untuk menghapus konten yang tidak pantas dan bahkan mencari informasi yang berkaitan dengan akun pengguna. Kami menyaksikan banyak contoh upaya untuk menyensor Internet mulai dari penangkapan kartunis Aseem Trivedi dan pemblokiran situs ini hingga pemblokiran situs oleh ISP karena masalah privasi, penangguhan akun Twitter yang diduga karena menyebarkan desas-desus selama kekerasan Assam baru-baru ini dan bahkan penangkapan atas posting di situs jejaring sosial. Sementara India termasuk dalam kategori 'bebas sebagian', dalam hal kebebasan Internet, peningkatan upaya pengawasan dan penyensoran telah menimbulkan kekhawatiran di antara badan pengawas Internet di seluruh dunia.

7.3 SENSOR MELALUI PEMBLOKIRAN

Amerika Serikat – sebuah negara yang telah menyaksikan protes luas terhadap RUU yang berusaha untuk mengekang kebebasan Internet – sebagian besar tetap bebas dari sensor Internet seperti yang terlihat dan dipraktikkan di negara-negara di seluruh dunia. Kami telah menyaksikan pertempuran yang dipublikasikan secara luas melawan tagihan kontroversial seperti Stop Online Piracy Act (SOPA), Anti-Counterfeiting Trade Agreement (ACTA), Cyber Intelligence Sharing and Protection Act (CISPA), PROTECT IP Act (PIPA). Undang-undang ini, jika mulai berlaku, akan berdampak tidak hanya di AS, tetapi juga banyak negara lain di dunia. Gerakan anti-SOPA khususnya mendapatkan dukungan dari situs-situs populer seperti Google, Wikipedia, Reddit, Mozilla, dll. karena mereka menutup situs mereka selama 24 jam. Netizen yang waspada dan aktivis pro-Internet memastikan bahwa RUU ini tidak menjadi kenyataan. Apa yang mungkin berperan adalah kehadiran Lembah Silikon dan fakta bahwa AS adalah rumah bagi semua perusahaan teknologi besar dunia. Kekhawatiran ekonomi memastikan bahwa raksasa teknologi ini memiliki suara dalam proses tersebut. Namun, ada peningkatan pemantauan situs jejaring sosial dalam beberapa tahun terakhir. Misalnya, situs mikroblog Twitter mengeluarkan permintaan untuk mengakses data pribadi pengguna, terutama yang terkait dengan organisasi seperti WikiLeaks dan bahkan gerakan Occupy Wall Street. Insiden

lain yang cukup menimbulkan kehebohan dan kecaman adalah inisiatif Departemen Kepolisian New York untuk memantau aktivitas online kelompok mahasiswa Muslim, yang menurut laporan berlangsung sejak 2006.

Mesir: Peran Internet dalam membantu revolusi muncul selama kerusuhan sipil di Mesir, ketika negara itu turun ke jalan dalam upaya untuk mengakhiri rezim tirani selama 30 tahun dari Presiden Hosni Mubarak. Apa yang membantu orang biasa yang berperang melawan pihak berwenang adalah anonimitas yang disediakan oleh Internet, karena digunakan secara menyeluruh sebagai alat untuk menyebarkan informasi tentang kegiatan di lapangan, menggalang pendukung dan yang paling penting, membawa ke dunia suara menentang kekejaman rezim. Tentu saja, pemerintah dengan cepat bertindak dan berusaha untuk memblokir Internet, tetapi sebagian besar tidak berhasil melakukannya.

Internet memainkan peran penting dalam revolusi sehingga revolusi Mesir secara populer dijuluki sebagai Revolusi Facebook. Seorang karyawan Google Wael Ghonim, yang mendirikan halaman Facebook yang mengutuk kematian seorang pemuda Mesir di tangan polisi, menjadi wajah revolusi. Dia ditangkap oleh pihak berwenang saat dia mendesak orang untuk bergabung dengan revolusi melalui jejaring sosial. Penangkapannya dan pembebasan selanjutnya menarik perhatian media di seluruh dunia. Ini mengumpulkan lebih banyak dukungan untuk revolusi dan membangun tekanan pada otoritas Mesir. Pasca revolusi, pemerintahan militer saat ini tidak mau mengambil risiko. Ini mempertahankan kontrol atas Internet dan media sosial pada khususnya. Ini memiliki alat pemantauan untuk mengawasi aktivitas online para pengguna internetnya. Beberapa kasus aktivis online dan blogger yang menghadapi kemarahan pihak berwenang telah muncul dalam setahun terakhir. Efek lain dari revolusi Mesir adalah bahwa hal itu telah menyebabkan peningkatan sensor di Internet oleh pemerintah di banyak negara Timur Tengah seperti Arab Saudi.

Pakistan: Tetangga India, Pakistan, juga terhuyung-huyung di bawah meningkatnya kasus sensor Internet. Insiden pemblokiran situs terus meningkat. Sementara sebagian besar tindakan keras dilakukan terhadap konten pornografi di web, semakin meningkat, tindakan itu juga dilakukan untuk memblokir situs-situs yang tidak menimbulkan ancaman nyata dan tampaknya bermotivasi politik. Misalnya, ia memblokir situs web majalah populer 'Rolling Stone' yang menyatakan bahwa majalah itu berisi foto-foto wanita berpakaian minim. Tetapi alasan sebenarnya bisa jadi adalah artikel yang diterbitkan di majalah yang menyoroti kenaikan pengeluaran militer. Facebook juga diblokir sementara karena kontroversi kontes 'Draw Mohammed Day'. Apa yang membuat berita baru-baru ini adalah pemblokiran dan pemblokiran ulang YouTube berikutnya. Situs tersebut dilarang selama lebih dari seratus hari karena film anti-Islam 'Innocence of Muslims', yang memicu banyak kemarahan di seluruh dunia. Baru-baru ini, ketika diblokir, banyak saluran media menunjukkan bahwa video yang menyebabkan kehebohan seperti itu, karena situs tersebut diblokir pada awalnya, masih dapat diakses di situs tersebut. Hal ini mengakibatkan pihak berwenang memblokir situs lagi. Menurut laporan, pihak berwenang Pakistan juga berencana untuk menerapkan sistem penyaringan dan pemblokiran URL otomatis nasional.

7.4 SENSOR & PENYARINGAN SELEKTIF

Penyensoran konten internet dapat dilakukan dalam berbagai bentuk dan rentang dari pemerintah yang memblokir penyebaran opini politik hingga memasukkan situs web pornografi dan bajak laut ke dalam daftar hitam. Inisiatif Terbuka adalah kolaborasi antara tiga kelompok – Lab Warga di sekolah urusan global Munk Universitas Toronto, pusat Internet & masyarakat Berkman Universitas Harvard, dan Grup SecDev di Ottawa – yang menyelidiki penyaringan internet di seluruh dunia.

Peneliti utama ONI dan direktur Citizen Lab Ronald Deibert mengatakan: Awalnya dan mungkin masih sebagian besar, pornografi adalah konten yang paling banyak ditargetkan dan juga yang paling dibenarkan oleh negara. Sebagian besar negara, jika mereka akan terlibat dalam sensor internet, mulai dengan berbicara tentang kategori luas konten yang tidak pantas. Tetapi apa yang kami temukan selama dekade terakhir adalah spektrum konten yang ditargetkan untuk difilter telah berkembang untuk memasukkan konten politik dan konten terkait keamanan, terutama di rezim otoriter. Cakupan dan skala konten yang ditargetkan untuk pemfilteran telah berkembang.

Untuk setiap negara, ONI melihat empat kategori pemfilteran berikut dan memberi masing-masing peringkat mulai dari "Tidak ada bukti pemfilteran" hingga "Pemfilteran meresap": Politik – konten yang menentang pemerintah saat ini atau kebijakannya; juga dapat berhubungan dengan hak asasi manusia, kebebasan berekspresi, hak minoritas atau gerakan keagamaan

- Sosial – konten yang mungkin dianggap menyinggung oleh masyarakat umum seperti seksualitas, perjudian, obat-obatan terlarang, dll
- Konflik/keamanan – Konten yang terkait dengan konflik bersenjata, sengketa perbatasan, militant kelompok dan gerakan separatis
- Alat Internet – Alat yang memungkinkan pengguna untuk berkomunikasi dengan orang lain, menghindari penyaringan atau yang menyediakan layanan. Setiap negara kemudian diklasifikasikan dalam hal konsistensi – seberapa konsisten topik ini disaring di seluruh penyedia layanan internet – dan transparansi – seberapa terlihat proses situs mana yang diblokir dan apakah pengguna dapat melihat apa yang ada di daftar hitam.

Menurut data ONI, Iran berada di peringkat terburuk, dengan penyaringan "menembus" dalam kategori alat politik, sosial dan internet dan "substansial" untuk penyaringan konflik/keamanan. Diuji pada tahun 2011, penyaringan Iran dinilai sebagai "sangat" konsisten dan memiliki transparansi "sedang". Bahkan presiden negara itu tidak kebal terhadap daftar hitam – dilaporkan pada bulan Februari tahun ini bahwa sensor telah memblokir akses ke beberapa situs berita yang mendukung Ahmadinejad menjelang pemilihan parlemen pada bulan Maret. Lebih buruk lagi, Iran telah mengusulkan internet nasional, yang akan meningkatkan cengkeraman pemerintah atas koneksi individu tetapi juga membatasi pengguna asing mengakses situs web Iran. Selain itu, individu juga diwajibkan untuk memberikan informasi pribadi bahkan untuk menggunakan warnet.

Setelah Iran adalah China, yang memiliki penyaringan politik dan konflik/keamanan yang "menyeluruh", bersama dengan alat internet "substansial" dan penyaringan sosial. Selain penyaringan yang sangat konsisten, China juga memiliki skor transparansi yang lebih rendah

daripada Iran. Pada 12 April, pengguna China terputus dari semua situs web asing, mungkin karena konfigurasi ulang dari apa yang disebut "firewall hebat".

Sementara itu, pihak berwenang telah menutup 42 situs web sejak Maret tahun ini. "Pasar untuk teknologi penyaringan telah berkembang di seluruh dunia; apa yang dimulai sebagai pasar yang terutama berorientasi pada lingkungan perusahaan di barat kini telah menjadi bisnis besar yang berkembang bagi pemerintah," kata Deibert.

Penelitian kami mengidentifikasi banyak perusahaan – kebanyakan perusahaan Silicon Valley – yang telah menyediakan produk dan layanan kepada rezim yang telah melanggar hak asasi manusia. Pasar untuk jenis teknologi yang digunakan untuk menerapkan kontrol ini tumbuh lebih canggih.

Namun, Deibert merasa pemerintah beralih dari daftar hitam situs web yang tersebar luas untuk menyaring dan menuju apa yang ONI sebut "penyaringan generasi berikutnya," yang mencakup pengawasan yang ditargetkan dan penyaringan "tepat waktu", atau penyaringan sementara konten hanya jika itu berharga – untuk misalnya saat pemilu. "Kami melihat tren menjauh dari sensor internet tradisional dan menuju kontrol generasi berikutnya," katanya. "Masa depan tidak terletak pada firewall yang hebat, tetapi pada cara negara-negara seperti Iran datang untuk menyaring konten."

7.5 SENSOR & WTO

China dan pemerintah lain yang terlibat dalam sensor internet yang membatasi akses ke informasi dari negara lain melanggar komitmen WTO mereka, Google berpendapat dalam makalah posisi baru. Memperingatkan bahwa "manfaat ekonomi transformatif dari Internet berada di bawah ancaman" dari pembatasan arus informasi yang diberlakukan pemerintah, perusahaan tersebut mendesak masyarakat internasional untuk "mengambil tindakan untuk memastikan arus informasi online yang bebas."

Google: GATS mencakup pembatasan internet

Keputusan Badan Banding WTO, seperti salah satu peraturan China yang berkaitan dengan impor berbagai produk media, "menunjukkan bahwa pembatasan informasi tunduk pada disiplin GATS," kata surat kabar itu.

Di bawah ketentuan GATS untuk non-diskriminasi, Google mengatakan, perusahaan asing harus diperlakukan tidak kurang baik daripada perusahaan domestik, dan pemasok layanan asing harus memiliki "akses yang wajar dan non-diskriminatif ke jaringan telekomunikasi publik, termasuk untuk memindahkan informasi di dalam dan lintas batas. " Pengecualian yang dijabarkan dalam GATS mengharuskan pemerintah untuk secara jelas membenarkan setiap pengurangan, dan menerapkannya dengan cara yang tidak diskriminatif.

"Sekarang terserah anggota [WTO] lainnya untuk memastikan bahwa pengecualian tidak menjadi aturan," kata surat kabar itu, mendesak pemerintah untuk melindungi "hak anggota untuk mengejar tujuan kebijakan yang sah sambil mencegah penerapan luas pengecualian yang akan merusak nilai GATS."

Google telah terkenal bentrok dengan Beijing atas kebijakan sensor internetnya. Itu menarik diri dari China awal tahun ini, setelah periode di mana mereka menyensor hasil pencarian di China dalam upaya untuk bekerja dengan Beijing. Dalam surat kabar tersebut, Google mengatakan bahwa pada bulan Oktober 2007, para pejabat China, yang marah atas

keputusan Kongres AS untuk memberikan penghargaan kepada Dalai Lama, mencurangi yang disebut 'firewall hebat' sehingga pengguna yang ingin mengakses mesin pencari yang berbasis di AS malah dikirim ke Baidu, mesin pencari milik Cina.

China bukanlah satu-satunya negara yang bersalah karena berusaha menyensor internet. Makalah itu mengatakan bahwa "lebih dari 40 pemerintah telah melembagakan pembatasan arus informasi berskala luas di internet," menggambarkan pemblokiran YouTube dan blog serta situs jejaring sosial di berbagai negara mulai dari.

Menyerukan "agenda perdagangan internet abad ke-21": Menguraikan apa yang disebutnya sebagai "agenda perdagangan Internet abad ke-21," Google meminta pemerintah di AS, Uni Eropa, dan di tempat lain untuk mengambil "langkah konkret untuk memastikan bahwa aturan di generasi berikutnya perjanjian perdagangan mencerminkan tantangan baru perdagangan Internet."

Sebagai contoh dari apa artinya ini, Google memuji teks perjanjian perdagangan bebas (FTA) Korea-AS yang belum selesai karena memasukkan ketentuan yang mengikat kedua negara untuk "berusaha menahan diri dari memaksakan atau mempertahankan hambatan yang tidak perlu terhadap arus informasi elektronik. lintas batas," karena pentingnya arus informasi untuk memfasilitasi perdagangan. Ke depan, kata Google, pemerintah pertama-tama harus "menutup kesenjangan dalam kerangka WTO yang ada untuk memastikan bahwa semua disiplin GATS berlaku untuk semua perdagangan Internet." Ini menyerukan negosiasi perdagangan bilateral dan multilateral baru untuk mencakup dan memasukkan "aturan baru yang mencerminkan ekonomi informasi saat ini." "Arus informasi yang bebas harus ada di atas meja" dalam negosiasi layanan Putaran Doha, menurut surat kabar itu. Dikatakan bahwa proposal yang ada pada layanan komputer dan telekomunikasi oleh AS, Kanada, Jepang, dan Uni Eropa "akan mulai merasionalisasi dan meningkatkan kepastian penjadwalan layanan internet." Pada akhirnya, "komitmen babak baru akan diperlukan untuk memastikan bahwa semua disiplin GATS berlaku untuk semua aktivitas ekonomi di internet."

Makalah itu mencatat bahwa UE memiliki "peluang untuk memajukan agenda perdagangan Internet" dalam pembicaraan perjanjian perdagangan bebas yang sedang berlangsung, seperti dengan India dan Kanada. Pembicaraan perjanjian perdagangan Kemitraan Trans-Pasifik memberi AS kesempatan serupa dengan sejumlah negara dari sekitar Lingkar Pasifik. Prosedur aksesi WTO juga ditunjuk sebagai contoh di mana tekanan dapat diberikan pada Rusia dan beberapa negara Timur Tengah untuk melonggarkan pembatasan berat yang mereka tempatkan pada penggunaan internet.

Hancurkan firewall ini?: Google bukan kelompok pertama yang menyerukan penggunaan aturan WTO untuk menyerang kebijakan sensor internet. Koalisi Amandemen Pertama California, sebuah kelompok advokasi kebebasan berekspresi, telah mengajukan petisi kepada kantor perwakilan perdagangan AS untuk memulai proses sengketa WTO dengan China atas pembatasan internetnya. 'Firewall yang hebat', menurutnya, adalah penghalang akses pasar yang membuat hampir tidak mungkin bagi perusahaan internet asing seperti situs lelang online eBay untuk melakukan bisnis di China, demi keuntungan para pesaing China mereka. Hingga Januari tahun ini, kantor USTR mengatakan belum mengambil keputusan tentang bagaimana menangani petisi tersebut. Pada saat publikasi pada hari Rabu, terlalu dini di Washington untuk menghubungi pejabat AS untuk berkomentar. pelaporan

ICTSD; "Google Melihat Pelanggaran Aturan dalam Pembatasan Akses Internet," NEW YORK TIMES, 17 November 2010.

7.6 PERJUDIAN ONLINE DIKENAKAN SENSOR

Dengan berkembangnya internet, industri judi online berkembang sangat pesat. Ekspansi cepat ini telah menimbulkan undang-undang permainan anti-Internet dari pemerintah negara bagian dan federal, bersama dengan pengaturan mandiri dalam industri kartu kredit. Alasan utama untuk menghambat perjudian online termasuk peningkatan masalah perjudian, akses anak-anak ke situs perjudian, penipuan melalui Internet, dan kerusakan moral (Manter 2003; Smith 2002). Sifat seperti video game dari kasino virtual sering menyulitkan para penjudi untuk menahan godaan untuk berjudi di internet (Kish 1999). Dalam lingkungan online, perjudian bermasalah dapat diperburuk karena penjudi online tetap anonim dan mungkin kehilangan jejak berapa banyak uang yang dimenangkan atau hilang karena, sebagian, karena uang digital tidak berwujud (Manter 2003). Perjudian di bawah umur dapat terjadi karena anak-anak dan remaja memiliki akses mudah ke situs perjudian tanpa meninggalkan rumah mereka (Kish 1999). Karena operasi perjudian lepas pantai berada di luar jangkauan undang-undang peraturan A.S., penjudi online terus menderita akibat kesalahan operator situs lepas pantai yang curang. Misalnya, kerugian penjudi online langsung dipotong dari akun online mereka, sementara kemenangan mereka seringkali tidak dikreditkan (Keller 1999). Pendukung peraturan perjudian internet percaya bahwa peraturan akan melindungi konsumen dari ancaman penipuan, kecanduan, kebangkrutan, dan kerusakan moral, serta dari bahaya taruhan online yang tidak dikenai pajak (Mainelli 2000).

Menanggapi kekhawatiran utama ini, Senat mengesahkan Undang-Undang Larangan Perjudian Internet tahun 1999 untuk melarang semua game online (Birnbaum 2000). Selain itu, Undang-Undang Penegakan Perjudian Internet disahkan oleh Dewan Perwakilan Rakyat pada tahun 2002 untuk mencegah penggunaan kartu kredit, cek, dan transfer dana elektronik untuk membayar taruhan interaktif (Smith 2002). Untuk aktivitas perjudian online, konsumen biasanya mendaftar di suatu situs dan menyetor uang untuk membuka rekening dengan menggunakan kartu kredit atau melakukan pembayaran melalui layanan uang tunai digital seperti PayPal dan NETeller (McAleavy 2002). Menanggapi upaya legislatif, perusahaan kartu kredit besar mengumumkan bahwa mereka akan melarang penggunaan kartu kredit mereka dalam transaksi moneter antara penjudi dan bisnis perjudian online. eBay, yang membeli PayPal, juga menyatakan akan melarang layanan memproses transaksi perjudian online (McAleavy 2002). Sederhananya, perjudian online adalah ilegal menurut undang-undang federal yang ada di Amerika Serikat.

Perdebatan mengenai regulasi konten Internet dan perlindungan anak di bawah umur tidak terbatas pada situs perjudian. Situs komersial yang mempromosikan permainan komputer kekerasan telah menimbulkan banyak kekhawatiran dari orang tua, pendidik, dan legislator (Simons 1999; Tribe 1999). Sebuah survei yang dirilis oleh Entertainment Software Association (2004) menunjukkan bahwa orang Amerika mengidentifikasi video, PC, dan permainan berbasis Internet sebagai bentuk hiburan favorit mereka, dibandingkan dengan menonton TV atau menonton film. Dengan semakin populernya permainan ini, para kritikus khawatir bahwa anak-anak atau remaja memiliki akses tak terbatas ke situs-situs permainan

Internet yang menampilkan kekerasan interaktif. Mereka menyalahkan komputer atau video game kekerasan karena membuat gamer tidak peka terhadap pertumpahan darah, atau karena mendorong perilaku kekerasan. Menanggapi kekhawatiran ini, serta kemarahan publik atas kekerasan di sekolah, FTC dan Departemen Kehakiman mendesak penyelidikan terhadap praktik pemasaran industri hiburan yang ditujukan untuk anak-anak dan remaja dan studi tentang hubungan antara perilaku agresif dan konsumsi hiburan kekerasan. (Broder 1999; Wallace 1999).

Konsekuensi negatif dari permainan komputer di beberapa bidang: aktivitas fisik, pendidikan, dan kesehatan psikologis. Sebagai contoh, penelitian telah menunjukkan bahwa jumlah permainan komputer yang berlebihan dapat menyebabkan kurangnya latihan fisik dan kecanduan (Griffiths 1997). Para peneliti khawatir bahwa permainan komputer yang berlebihan oleh anak-anak sekolah dapat menyebabkan mereka mengabaikan pekerjaan rumah mereka dan kurang tertarik pada pendidikan mereka, meskipun kekhawatiran ini sebagian besar tetap tidak berdasar (Creasey dan Myers 1986; Griffiths 1997). Para peneliti juga telah melaporkan bukti yang menunjukkan bahwa permainan komputer kekerasan di antara anak-anak dan remaja dapat meningkatkan priming dan elaborasi jaringan pemikiran agresif (Anderson dan Dill 2000; Berkowitz 1984, 1990), melemahkan hambatan terhadap perilaku agresif, dan meningkatkan penerimaan penggunaan kekerasan untuk menyelesaikan konflik (Berkowitz dan Green 1967; Dill dan Dill 1998).

Kekhawatiran tentang potensi efek negatif dari situs web perjudian dan permainan ini merupakan inti dari perdebatan sensor. Studi sebelumnya berpendapat bahwa dukungan untuk regulasi pemerintah atas konten media dihasilkan dari pesan yang dianggap berbahaya (Rucinski dan Salmon 1990). Upaya untuk membatasi konten media jarang didasarkan pada bukti penelitian yang menunjukkan dampak negatif dari pesan-pesan ini. Sebaliknya, mereka didasarkan terutama pada persepsi tentang efek berbahaya dari pesan pada orang lain - publik "tertipu" (Gunther 1995; McLeod, Eveland, dan Nathanson 1997; Rojas, Shah, dan Faber 1996). Argumen ini dijelaskan oleh efek orang ketiga di bidang teori komunikasi massa (Davison 1983). Efek orang ketiga baru-baru ini disebut sebagai "pengaruh pengaruh yang diduga" (Gunther dan Storey 2003, hal.199), yang memasukkan gagasan bahwa orang merasakan beberapa pengaruh komunikasi pada orang lain dan, sebagai hasilnya, berubah sikap atau perilaku mereka sendiri. Efek orang ketiga mengklaim bahwa orang merasakan dampak dari pesan yang mungkin berbahaya lebih besar pada orang lain daripada pada diri mereka sendiri, dan dengan demikian mereka bersedia menyensor pesan-pesan ini (Davison 1983).

7.7 SENSOR & HUKUM PERDAGANGAN

Internet adalah pasar global. Perkembangan pesat Internet, dan terutama perdagangan berbasis Internet, sebagian besar terjadi di luar kerangka kerja peraturan perdagangan standar yang mencakup sebagian besar bentuk perdagangan lintas batas lainnya. Karena ukuran pasar Internet telah tumbuh, dan sebagai kontribusi mereka terhadap ekonomi secara keseluruhan telah menjadi lebih jelas, lebih banyak perhatian telah diberikan kepada masalah peraturan, seperti tindakan pembatasan perdagangan, merusak iklim perdagangan dan investasi di bidang perdagangan. e-commerce, layanan berbasis informasi

dan transmisi online. Baru-baru ini, Banyak upaya untuk menegakkan tindakan tersebut telah disorot di media: Pada tahun 2009, pemilihan Iran dijuluki sebagai revolusi 'Twitter' setelah layanan online yang coba diblokir oleh pihak berwenang; China awalnya berencana untuk memperkenalkan perangkat lunak penyaringan yang disebut Green Dam Youth Escort pada setiap PC yang dijual di negara itu, dan juga telah memblokir mesin pencari populer dan situs streaming video pada beberapa kesempatan. Pemerintah China telah mengumumkan larangan distribusi berita oleh kantor berita asing di China, kecuali badan milik negara, Xinhua, yang melarang Reuters, AP, Bloomberg, AFP, Kyodo, untuk menjual konten ke media China. Masalah muncul dari fakta sederhana bahwa Internet tidak menghormati batas-batas nasional dan layanan online yang disediakan di satu titik di dunia, pada prinsipnya, dapat diakses di titik lain. Pemerintah, yang lebih suka bahwa bagian tertentu dari informasi layanan harus tetap tidak dapat diakses dari populasi, tidak dapat bertindak di luar yurisdiksinya menggunakan cara penegakan tradisional: Siapa pun, dengan sedikit atau tanpa sarana, memiliki jangkauan global instan tanpa masuk pasar tradisional hambatan seperti investasi fisik, distributor, real estat, dan infrastruktur – dan yang lebih penting, semua instrumen peraturan (seperti izin, lisensi, dan pengawasan) yang didasarkan pada hambatan tersebut.

7.8 SENSOR INTERNET-POSISI AS

Pemerintah AS telah memberlakukan dua undang-undang Federal yang dimaksudkan untuk menyensor konten online yang menyinggung. Tak satu pun dari undang-undang ini berlaku pada Maret 2002. Undang-undang pertama (CDA) dibatalkan oleh Mahkamah Agung AS dengan alasan Amandemen Pertama. Undang-undang kedua (COPA), yang lebih fokus secara sempit dan hanya mencakup komunikasi yang dibuat untuk tujuan komersial di World Wide Web, adalah subjek dari perintah Pengadilan (juga berdasarkan Amandemen Pertama) yang mencegah penegakannya sambil menunggu keputusan Mahkamah Agung. Keputusan Pengadilan diperkirakan akan dijatuhkan pada akhir tahun 2002. Sejak 1996, empat negara bagian AS, New York, New Mexico, Michigan, dan Virginia telah mengesahkan undang-undang sensor Internet yang membatasi/melarang distribusi online materi yang dianggap "berbahaya bagi anak di bawah umur". Hukum-hukum ini telah dijatuhkan atas dasar Konstitusi.
Informasi tentang dua undang-undang Federal disediakan di bawah ini.

Communications Decency Act (CDA): CDA disahkan pada Februari 1996. Pada bulan yang sama, Pengadilan AS mengeluarkan perintah penahanan yang mencegah penegakannya. Pada bulan Juni 1996, sebuah panel hakim federal di Philadelphia memutuskan CDA inkonstitusional. Pada bulan Juni 1997, Mahkamah Agung AS menjatuhkan CDA dengan alasan melanggar Amandemen Pertama.

Informasi singkat berikut tentang CDA diambil dari Pengadilan Banding AS untuk keputusan Sirkuit Ketiga (Feb 2000) tentang COPA:
CDA melarang pengguna Internet menggunakan Internet untuk mengomunikasikan materi yang, menurut standar komunitas kontemporer, akan dianggap menyinggung anak di bawah umur di bawah delapan belas tahun. Dalam membatasi pengguna Internet, CDA memberikan dua pembelaan afirmatif untuk penuntutan; (1) penggunaan kartu kredit atau sistem verifikasi usia lainnya, dan (2) setiap upaya itikad baik untuk membatasi akses oleh anak di bawah umur.Dalam menyatakan bahwa CDA melanggar Amandemen Pertama, Mahkamah

Agung menjelaskan bahwa tanpa mendefinisikan istilah kunci undang-undang tersebut inkonstitusional Selain itu, Pengadilan mencatat bahwa luasnya CDA "sepenuhnya belum pernah terjadi sebelumnya" dalam hal, misalnya, "tidak terbatas pada pidato komersial atau entitas komersial . . . [melainkan] larangan terbuka mencakup semua entitas dan individu nirlaba yang memposting pesan tidak senonoh atau menampilkannya di komputer mereka sendiri.

Lebih lanjut, Pengadilan menjelaskan bahwa, sebagaimana diterapkan pada Internet, kriteria standar komunitas akan secara efektif berarti bahwa karena semua komunikasi Internet tersedia untuk audiens di seluruh dunia, isi pesan yang disampaikan akan dinilai berdasarkan standar komunitas yang paling mungkin. tersinggung dengan isinya. Akhirnya, sehubungan dengan pembelaan afirmatif yang disahkan oleh CDA, Pengadilan menyimpulkan bahwa pembelaan semacam itu tidak akan layak secara ekonomi untuk sebagian besar penerbit Web non-komersial, dan bahwa bahkan sehubungan dengan penerbit komersial, teknologi tersebut belum terbukti efektif dalam melindungi anak di bawah umur. dari bahan berbahaya. Akibatnya, Pengadilan menyatakan bahwa CDA tidak dirancang sedemikian sempit untuk mencapai kepentingan pemerintah yang mendesak dalam melindungi anak di bawah umur, dan bahwa CDA tidak memiliki ketepatan yang diperlukan Amandemen Pertama ketika undang-undang mengatur isi pidato."

Child Online Protection Act (COPA): COPA adalah sekuel CDA dan bertujuan untuk menghindari cacat konstitusional CDA. COPA mencakup komunikasi yang dibuat untuk tujuan komersial di World Wide Web. Ini mengharuskan penerbit Web komersial untuk memastikan bahwa anak di bawah umur tidak mengakses "materi yang berbahaya bagi anak di bawah umur" di situs Web mereka.

COPA disahkan pada 21 Oktober 1998. Pada 20 November 1998, Pengadilan Distrik AS untuk Distrik Timur Pennsylvania mengeluarkan perintah penahanan sementara terhadap penegakan hukum dan kemudian, pada 1 Februari 1999, mengeluarkan perintah yang mencegah pemerintah menegakkan hukum. hukum. Pada tanggal 22 Juni 2000, Pengadilan Banding AS untuk Sirkuit Ketiga menguatkan perintah pengadilan yang lebih rendah. Pengadilan menyatakan dalam kesimpulannya bahwa "Karena keterbatasan teknologi saat ini, COPA - upaya pujian Kongres untuk mencapai tujuan yang menarik untuk melindungi anak di bawah umur dari materi berbahaya di World Wide Web - lebih mungkin ditemukan tidak konstitusional sebagai overbroad pada pahala." Keputusan itu diajukan banding ke Mahkamah Agung AS dan keputusan Pengadilan itu diharapkan akan dijatuhkan pada akhir tahun 2002.

Ikhtisar ketentuan COPA termasuk dalam keputusan Pengadilan Banding Februari 2000:

'COPA ... mencoba untuk "mengatasi[ ] keprihatinan khusus yang diajukan oleh Mahkamah Agung" dalam membatalkan CDA. COPA melarang individu atau entitas dari: "dengan sadar dan dengan pengetahuan tentang karakter materi, dalam perdagangan antarnegara bagian atau asing melalui World Wide Web, membuat komunikasi apa pun untuk tujuan komersial yang tersedia untuk anak di bawah umur dan yang termasuk materi apa pun yang berbahaya bagi anak di bawah umur."

Sebagai bagian dari upayanya untuk menyembuhkan cacat konstitusional yang ditemukan dalam CDA, Kongres berusaha untuk mendefinisikan sebagian besar istilah kunci COPA. COPA mencoba, misalnya, untuk membatasi ruang lingkupnya pada materi di Web daripada di Internet secara keseluruhan;4 hanya menargetkan komunikasi Web yang dibuat untuk "tujuan komersial";5 dan membatasi ruang lingkupnya hanya pada materi yang dianggap " berbahaya bagi anak di bawah umur."

Berdasarkan COPA, apakah materi yang dipublikasikan di Web "berbahaya bagi anak di bawah umur" diatur oleh pengujian tiga bagian, yang masing-masing harus ditemukan sebelum kewajiban dapat dilampirkan:

a rata-rata orang, menerapkan standar komunitas kontemporer, akan menemukan, mengambil materi secara keseluruhan dan sehubungan dengan anak di bawah umur, dirancang untuk menarik, atau dirancang untuk memanjakan, kepentingan prurient;

b menggambarkan, menggambarkan, atau mewakili, dengan cara yang terang-terangan menyinggung terhadap anak di bawah umur, tindakan seksual atau kontak seksual aktual atau simulasi, tindakan seksual normal atau menyimpang yang sebenarnya atau yang disimulasikan, atau pameran alat kelamin atau payudara wanita pasca-puber yang cabul ; dan

c secara keseluruhan, tidak memiliki nilai serius, sastra, seni, politik, atau ilmiah untuk anak di bawah umur.

COPA juga memberikan pembelaan afirmatif kepada penerbit Web yang tunduk pada undang-undang tersebut. Jika penerbit Web" telah membatasi akses oleh anak di bawah umur ke materi yang berbahaya bagi anak di bawah umur" melalui penggunaan "kartu kredit, rekening debit, kode akses orang dewasa, atau nomor identifikasi pribadi orang dewasa . . . sertifikat digital yang memverifikasi usia . . . . atau dengan tindakan wajar lainnya yang layak di bawah teknologi yang tersedia," maka tidak ada kewajiban yang akan melekat pada penerbit Web meskipun anak di bawah umur harus mendapatkan akses ke materi terbatas di bawah COPA.' Klasifikasi Offline: Di AS, film, video, dan permainan komputer tidak diwajibkan secara hukum untuk diklasifikasikan sebelum pameran, penjualan, atau penyewaan. Sistem pemeringkatan sukarela non-pemerintah yang didirikan dan dikelola secara luas digunakan.

7.9 MOTIVASI PENYENSORAN

Karena penyensoran sebagai sebuah fenomena setua peradaban itu sendiri, tidak mengherankan bahwa motivasi dan target penyensoran online tidak jauh berbeda dengan yang mempengaruhi media lain. Motivasi politik, untuk mengekang ide-ide kritis, kelompok oposisi dan kritik rezim, adalah hal biasa. Lalu lintas internet dipantau secara ketat dan situs-situs penting yang berbasis di luar negeri diblokir di banyak negara, termasuk, antara lain, Cina, Iran, Maladewa, Myanmar, Korea Utara, Suriah, Tunisia, Turki, Uzbekistan, Vietnam, dan lain-lain. Di Kuba, mengakses Internet sendiri merupakan tindakan ilegal, tanpa izin resmi yang sesuai. Subjek untuk sensor politik juga bisa berupa konflik etnis atau bersenjata. Di China misalnya, informasi yang berkaitan dengan Falun Gong, Taiwan, Lapangan Tiananmen atau gerakan kemerdekaan Tibet diblokir. Informasi tentang Korea Utara secara rutin disensor di Korea Selatan.

Lembaga penegak hukum di Rusia dan negara-negara CIS lainnya telah diberi kekuasaan untuk sepenuhnya memantau semua aktivitas Internet mengikuti pengalaman di Ukraina dan Georgia, di mana pihak oposisi berhasil memanfaatkan komunikasi modern untuk memulai pemberontakan rakyat. Tokoh politik juga merupakan subjek yang sensitif – layanan populer seperti layanan video streaming YouTube dan layanan blog telah ditutup di Turki karena mencemarkan nama baik Kemal Atatürk, bapak pendiri republik. Demikian pula, kritik terhadap Raja, lèse majesté, dilarang di Thailand secara online maupun offline (dan sering digunakan untuk menuntut pihak oposisi). Undang-undang Prancis dan Jerman yang menentang pemuliaan Nazisme dan penyangkalan holocaust ditegakkan secara online terhadap situs-situs yang dihosting di luar negeri, sementara kadang-kadang menikmati perlindungan konstitusional di negara lain.

Motivasi kedua untuk penyensoran adalah untuk alasan moral, berdasarkan apa yang masyarakat anggap tidak bermoral atau ilegal. Contohnya sangat banyak, dan biasanya menyangkut pornografi, perjudian, atau kegiatan kriminal. Pemblokiran situs asing atas dasar ini adalah hal biasa di banyak negara Muslim, di mana konten dewasa, perjudian, penyalahgunaan zat dan diskusi tentang banyak hal yang berkaitan dengan iman adalah dilarang (yang di Iran meluas ke diskusi tentang hak-hak perempuan). Sensor moral dengan alasan yang lebih sekuler juga ada: di Amerika Serikat, perjudian online adalah ilegal meskipun situsnya tidak diblokir. Situs yang terlibat dalam berbagi file ilegal dan mengunduh materi berhak cipta diblokir di beberapa negara, termasuk Cina dan Denmark, tetapi tetap dapat diakses di sebagian besar negara lain. Sebagian besar negara (termasuk mereka yang tidak menerapkan sensor sendiri) memblokir situs yang menawarkan pornografi anak.

Motif ketiga, meskipun lebih jarang, adalah untuk tujuan komersial. Contoh yang paling menonjol adalah Meksiko, di mana mantan operator milik negara, Telmex, memblokir operator berbasis Internet seperti Skype dan Vonage, menyediakan layanan voice-over IP (VoIP) yang murah. Meksiko telah ditemukan oleh WTO untuk mendiskriminasi operator telepon di AS dengan membebankan biaya yang berlebihan kepada operator AS untuk mengirimkan panggilan mereka ke Meksiko, yang disebut biaya interkonektivitas. Kasus serupa juga terjadi melalui VoIP, seperti Deutsche Telekom di Jerman dan beberapa perusahaan Prancis dan Inggris. China melakukan pembatasan serupa dengan hanya memberikan lisensi kepada dua operator domestik untuk menjalankan layanan VoIP. Sensor komersial mungkin juga diterapkan oleh aktor non-negara: Di China, Sanlu (produsen susu lokal utama) dikatakan telah membayar Baidu, mesin pencari terkemuka di China, Rp 3.750.000.000 untuk memblokir hasil pencarian yang terkait dengan kontaminasi melamin produk susu Sanlu.

7.10 STUDI KASUS

Seruan untuk pra-penyensoran konten di Media Sosial: Desember 2011 Menteri Komunikasi dan Teknologi Informasi Serikat India Kapil Sibal menyerukan media sosial besar termasuk Google, Facebook, Twitter antara lain untuk menyensor konten yang diunggah oleh penggunanya. Ini mengundang kritik luas dari netizen India dan media. Dia kemudian mengklarifikasi bahwa dia tidak bermaksud menyensor konten sebelumnya tetapi berarti bahwa perusahaan harus memiliki standar yang mencegah konten tersebut berada di ruang

mereka. Dia juga bersikeras bahwa perusahaan-perusahaan ini harus mengikuti hukum negara, yang berarti bahwa perusahaan media sosial harus mengikuti pembatasan kebebasan berbicara seperti yang dianggap oleh konstitusi. Konten yang melanggar masalah berikut dianggap sebagai pembatasan dan pelanggaran kebebasan berpendapat.

- Keamanan Negara
- Hubungan persahabatan dengan negara asing
- Pesanan publik
- Kesusilaan dan moralitas
- Penghinaan terhadap pengadilan
- Pencemaran nama baik
- Penghasutan untuk melakukan pelanggaran
- Kedaulatan dan integritas India.

Media di India tidak menikmati 'kebebasan pers' yang terpisah seperti yang diabadikan oleh konstitusi AS tetapi kebebasan pers dimasukkan ke dalam kebebasan berbicara dan berekspresi, sebuah hak fundamental. Namun, ada banyak pembatasan di media India. Misalnya, berita Radio sepenuhnya dilarang di India dengan 'Radio Seluruh India' milik Negara menikmati monopoli penuh atas penyiaran berita melalui radio. Internet sampai 2008 relatif gratis dan sensor oleh Pemerintah sporadis. Usul Sibal mendapat kecaman luas di kalangan netizen, terutama di Twitter.

Kasus Vinay Rai: Di tengah hiruk pikuk penyensoran Internet, perantara seperti Facebook, Google dan perusahaan lain menghadapi kejutan baru ketika Vinay Rai, editor surat kabar Urdu yang berbasis di Delhi, Akbari, mengajukan kasus terhadap mereka pada Desember 2011 karena mengizinkan konten yang tidak pantas di situs mereka. Rai telah mengirimkan contoh-contoh konten yang dia anggap sebagai konten yang menyinggung berbagai agama dan tokoh agama yang dia temukan di situs-situs perusahaan tersebut. Namun, Rai memilih untuk tidak berinteraksi dengan situs web terkait masalah ini. Dia menyatakan bahwa pemerintah adalah otoritas tertinggi untuk berurusan dengan perusahaan multinasional dalam hal-hal seperti ini. KUHP India memiliki ketentuan ketat terhadap promosi permusuhan agama di negara tersebut termasuk Pasal 153 (B), Bagian 298 antara lain.

Meskipun Google dan Facebook telah berargumen bahwa mereka tidak bertanggung jawab secara hukum atas konten yang diunggah oleh pengguna, hal-hal tidak terlihat cerah, berkat undang-undang cyber di India. Hasil dari kasus ini masih tertunda karena kasusnya masih di Pengadilan Tinggi Delhi. Vijayashankar menambahkan, "Vinay Rai tampaknya telah mengajukan kasus terhadap konten yang dapat melukai sentimen keagamaan masyarakat. Ada beberapa ketentuan kuat dalam undang-undang yang melarang menyakiti sentimen agama. Satu-satunya ketakutan yang saya miliki adalah pengadilan harus menjelaskan bahwa putusannya hanya untuk kasus ini saja dan bahwa hasil kasus tidak boleh dianggap sebagai preseden. Ada elemen besar kepentingan publik dalam masalah ini. Ini memiliki bahaya disalahartikan sebagai preseden yang akan mempengaruhi kebebasan kita ekspresi."

Pemerintah India meminta Google untuk menghapus konten 'ofensif': Ketika perdebatan tentang sensor Internet mencapai puncaknya, Google mengungkapkan data yang menunjukkan niat sebenarnya dari Pemerintah. Menurut Google, perusahaan menerima 68

permintaan penghapusan konten (termasuk 358 item secara keseluruhan) dari Pemerintah India pada paruh pertama tahun 2011 (Januari – Juni) di mana 51% dari permintaan dipatuhi. Alasannya berkisar dari pencemaran nama baik, keamanan nasional, kritik pemerintah antara lain. Menarik untuk dicatat bahwa dari semua permintaan, hanya satu yang dikaitkan dengan Keamanan Nasional, alasan utama yang dikutip untuk amandemen yang terjadi pada tahun 2008.

Pada April 2011, Center for Internet and Society, sebuah organisasi penelitian dan advokasi di India mengungkapkan bahwa Pemerintah India melarang sekitar 11 situs web yang menggunakan ketentuan seperti 69B, yang di atas memberikan kekuasaan besar kepada Pemerintah. Sementara Google menentang Pemerintah China yang menolak untuk mematuhi norma-norma sensor yang terakhir, itu tidak benar-benar menunjukkan semangat yang sama di India. Baru-baru ini, bulan ini, Pengadilan Tinggi Delhi menanggapi gugatan perdata yang diajukan oleh Aijaz Qasmi, seorang warga negara India yang memerintahkan Google untuk menghapus 'konten ofensif' dari situs mereka. Sebuah pernyataan yang dikeluarkan oleh Google berbunyi: "Langkah ini sesuai dengan kebijakan lama Google dalam menanggapi perintah pengadilan." Google telah menggunakan sensor diri dan mengklaim bahwa mereka akan menghormati hukum negara. Twitter juga telah menyatakan bahwa mereka akan menyensor tweet secara geografis.

Trivedi mengatakan, "Ini pasti akan terjadi. Perusahaan seperti Google, Facebook, dan lainnya adalah entitas bisnis. Mereka pada akhirnya akan tunduk pada undang-undang yang tidak adil ini. Pada akhirnya terserah warga India untuk melawan undang-undang yang tidak adil ini." Kovacs menambahkan bahwa, "Dengan membuat perantara bertanggung jawab atas konten yang diunggah oleh pengguna, Pemerintah memastikan bahwa sejumlah besar pengguna internet dapat dikendalikan dan ini berbahaya."

Hukum untuk ruang tanpa batas geografis

Jika Facebook adalah negara dengan jumlah pengguna di dalamnya, itu akan menjadi negara terbesar ketiga dalam hal populasi. Internet pada dasarnya telah menembus batas-batas geografis dan melambangkan pepatah Sansekerta Vasudaiva Kumtumbakam—dunia hanyalah satu keluarga. Untuk memberlakukan undang-undang yang berlaku untuk wilayah geografis tertentu ke ruang yang tidak mengenal geografi memang akan menjadi rumit. Sementara Google telah mengumumkan bahwa mereka akan menyensor konten yang diperlukan oleh hukum negara, konten yang sama di atas dapat diakses di negara lain. Ini adalah latihan yang sia-sia karena server proxy dapat digunakan untuk mengakses konten yang sama dari negara yang sama tempat konten tersebut dilarang.

7.11 RINGKASAN

Masalah sensor internet adalah masalah yang sangat diperdebatkan di seluruh dunia dan pemerintah menggunakannya sebagai alat untuk membatasi kebebasan berbicara dan berekspresi bahkan saya demokrasi yang kuat seperti India. Dalam unit ini konsep sensor internet, penyensoran melalui pemblokiran, penyensoran dan penyaringan selektif, penyensoran dan WTO, perjudian online menanggung penyensoran, penyensoran dan undang-undang perdagangan, posisi AS khususnya penyensoran, dan motivasi penyensoran

dibahas panjang lebar dengan sesuai. contoh dan ketentuan hukum yang relevan dari instrumen hukum nasional dan internasional.

7.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Penulis)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

7.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a Sensor internet I India dilakukan secara selektif oleh Pemerintah Pusat dan Negara Bagian.

b Hampir tidak ada batas di internet dan kita dapat membaca informasi dari negara yang sangat jauh.

c Sejak beberapa tahun terakhir, kasus Sensor Internet di India telah meningkat berlipat ganda.

d Sementara India termasuk dalam kategori 'bebas sebagian' dalam hal kebebasan Internet.

e Internet bukanlah tempat pasar global.

B. Isi Bagian yang Kosong:

i India mengadopsi Aturan TI baru, 2011, aturan ini ..... untuk perantara internet untuk menghapus konten yang tidak pantas .... menerima keluhan.

ii Laporan Transparansi Google menunjukkan meningkatnya permintaan dari pemerintah untuk menghapus.....dan bahkan mencari informasi yang berkaitan dengan..... .....

iii China dan pemerintah lain yang terlibat dalam sensor internet yang membatasi akses ke informasi dari negara lain melanggar.....

iv Dengan berkembangnya Internet,.....industri telah berkembang sangat pesat.

v ..... telah memberlakukan dua Hukum Federal yang dimaksudkan untuk menyensor konten online yang menyinggung.

7.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Salah

B.

1. Membuatnya Wajib, Dalam 36 jam
2. Konten yang Tidak Menyenangkan, Akun Pengguna
3. Komitmen WTO
4. Perjudian Daring
5. Pemerintah AS

7.15. Pertanyaan Terminal

1. Apa itu sensor internet?
2. Apa yang dimaksud dengan penyensoran melalui pemblokiran?
3. Apa itu sensor dan penyaringan selektif?
4. Definisikan sensor dan WTO.
5. Mendefinisikan sensor dan hukum perdagangan.

BAB 8
MASALAH PRIVASI DAN SEKURITAS ONLINE

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami masalah dan pokok bahasan yang terkait dengan Masalah Privasi dan Keamanan Online
- Memahami solusi yang tersedia terhadap Pelanggaran Privasi
- Memahami masalah teknis dan hukum yang terkait dengan Masalah Privasi dan Keamanan Online

8.1 PENGANTAR

Pertumbuhan penggunaan Internet yang menakjubkan di beberapa negara juga meningkatkan kekhawatiran tentang privasi. Kualitas yang membuat jaringan komputer menjadi alat yang ampuh untuk meningkatkan efisiensi dan standar hidup juga memberi mereka kekuatan luar biasa untuk mengumpulkan, menyimpan, atau mendistribusikan data medis, data keuangan, dan informasi pribadi atau biografis lainnya. Banyak individu dan kelompok konsumen menyerukan perlindungan privasi baru untuk Internet dan jaringan komputer lainnya.

Informasi pribadi yang mungkin menarik bagi bisnis atau orang-orang dengan tujuan jahat dihasilkan setiap kali orang menjelajahi Internet. Perusahaan, misalnya, dapat belajar banyak tentang peselancar Web yang mengunjungi situs web mereka. Menggunakan perangkat pelacak yang dikenal sebagai "cookies", perusahaan dapat melacak pembelian dan mengumpulkan data pribadi. Mereka dapat menggunakan informasi ini untuk menargetkan upaya pemasaran mereka pada konsumen individu atau kelompok konsumen. Sementara beberapa orang mungkin menyambut baik perhatian yang meningkat terhadap kebutuhan konsumen mereka, yang lain mungkin menganggapnya sebagai pelanggaran privasi mereka. Ada juga kekhawatiran yang berkembang tentang apa yang dilakukan toko online dan konvensional dengan pembelian atau data pribadi yang mereka kumpulkan selama transaksi. Di bawah tekanan dari konsumen, beberapa toko baru-baru ini mulai mengembangkan kebijakan privasi, tetapi kelompok konsumen mengatakan banyak dari kebijakan ini gagal.

Akhirnya, pasien dan pendukung konsumen ingin menetapkan aturan untuk berbagi data medis pribadi. Di setiap area ini, akan sulit untuk mencapai keseimbangan antara melindungi privasi dan memastikan aliran informasi dan data yang dapat meningkatkan kualitas hidup. Alat berbasis Internet yang sama yang dapat meningkatkan pendidikan, kesehatan, dan pemerintahan juga dapat menyebabkan kerusakan yang cukup besar bila digunakan untuk tujuan pencurian atau penipuan. Perusahaan dan pengguna komputer individu semakin terpengaruh oleh virus komputer dan skema untuk mencuri data atau identitas komputer. Perusahaan menghabiskan banyak waktu dan uang untuk melindungi jaringan dan data mereka. Jajak pendapat terbaru menunjukkan bahwa dua pertiga dari perusahaan Amerika telah mengalami beberapa dari "gangguan dunia maya".

Sumber daya yang dapat diarahkan untuk meningkatkan kapasitas Internet digunakan untuk menggagalkan penjahat dunia maya. Menurut sebuah artikel yang diterbitkan di Financial Times, biaya tahunan rata-rata per perusahaan dari gangguan ini melebihi dua juta dolar. Biro Investigasi Federal (FBI) memperkirakan kerugian tahunan industri dalam kisaran Rp 150.000 – Rp 225.000 miliar. Data terbaru memperkirakan bahwa pengeluaran di seluruh dunia untuk keamanan akan mencapai Rp 1.290.000 miliar pada tahun 2016 sebagai akibat dari meningkatnya kekhawatiran atas kejahatan dunia maya dari China, yang telah diprioritaskan oleh pemerintahan Obama (Info security, 2012). Gangguan layanan internet atau komputer telah menjadi masalah besar tidak hanya bagi perusahaan, tetapi juga bagi pemerintah, asosiasi, lembaga internasional, dan warga negara di seluruh dunia.

8.2 RISIKO DARING

Keamanan dunia maya, phishing, worm, firewall, Trojan horse, peretas, dan virus tampaknya menjadi berita setiap hari. Ditambah peringatan untuk memperbarui perlindungan virus Anda, waspada terhadap penipuan online, lindungi privasi Anda, dan lihat apa yang Anda klik ada di mana-mana. Tapi apa artinya semua ini? Dan apa yang dapat Anda lakukan untuk melindungi akses ke komputer Anda dan untuk melindungi diri Anda dan keluarga Anda? Apa ini semua tentang?

Langkah pertama dalam melindungi diri Anda sendiri adalah mengenali risikonya dan membiasakan diri dengan beberapa terminologi yang terkait dengan keamanan siber. Departemen Keamanan Dalam Negeri membuat daftar istilah ini: Peretas, penyerang, atau penyusup - Istilah-istilah ini diterapkan pada orang-orang yang berusaha mengeksploitasi kelemahan dalam perangkat lunak dan sistem komputer untuk keuntungan mereka sendiri. Meskipun niat mereka kadang-kadang cukup jinak dan hanya dimotivasi oleh rasa ingin tahu, tindakan mereka biasanya melanggar tujuan penggunaan sistem yang mereka eksploitasi. Hasil dapat berkisar dari kerusakan belaka (membuat virus tanpa dampak negatif yang disengaja) hingga berbahaya (mencuri atau mengubah informasi).

Kode berbahaya termasuk kode seperti virus, worm, dan trojan horse. Meskipun beberapa orang menggunakan istilah ini secara bergantian, mereka memiliki karakteristik unik:

- Virus - Jenis kode berbahaya ini mengharuskan Anda untuk benar-benar melakukan sesuatu sebelum menginfeksi komputer Anda. Tindakan ini dapat berupa membuka lampiran email atau membuka halaman web tertentu.
- Cacing - Cacing berkembang biak tanpa Anda melakukan apa pun. Mereka biasanya mulai dengan mengeksploitasi kerentanan perangkat lunak (cacat yang memungkinkan kebijakan keamanan perangkat lunak yang dimaksudkan untuk dilanggar). Kemudian setelah komputer korban terinfeksi, worm akan berusaha mencari dan menginfeksi komputer lain. Mirip dengan virus, worm dapat menyebar melalui email, situs web, atau perangkat lunak berbasis jaringan. Perbanyakan worm otomatis membedakannya dari virus.
- Kuda Troya - Program kuda Troya adalah perangkat lunak yang mengklaim melakukan satu hal sementara, pada kenyataannya, melakukan sesuatu yang berbeda di belakang

layar. Misalnya, sebuah program yang mengklaim akan mempercepat komputer Anda mungkin sebenarnya mengirimkan informasi rahasia Anda ke penyusup.

- Spyware - Perangkat lunak licik ini masuk ke komputer saat Anda mengunduh screensaver, game, musik, dan aplikasi lainnya. Spyware mengirimkan informasi tentang apa yang Anda lakukan di Internet ke pihak ketiga, biasanya untuk menargetkan Anda dengan iklan pop-up. Browser memungkinkan Anda untuk memblokir pop-up. Anda juga dapat menginstal anti-spyware untuk menghentikan ancaman ini terhadap privasi Anda.
- Mungkin mudah bagi Anda untuk mengidentifikasi orang yang dapat memperoleh akses fisik ke komputer Anda—anggota keluarga, teman sekamar, rekan kerja, anggota kru kebersihan, dan mungkin beberapa lainnya. Tetapi mengidentifikasi orang-orang yang dapat memperoleh akses jarak jauh ke komputer Anda menjadi jauh lebih sulit. Selama Anda memiliki komputer dan menghubungkannya ke jaringan atau internet, Anda rentan terhadap seseorang atau sesuatu yang mengakses atau merusak informasi Anda. Untungnya, Anda dapat mengembangkan kebiasaan yang membuatnya lebih sulit.
- Kunci atau log-off komputer Anda saat Anda jauh darinya. Ini mencegah orang lain menunggu Anda pergi dan kemudian duduk di depan komputer Anda dan mengakses semua informasi Anda.
- Agar benar-benar aman, putuskan sambungan komputer Anda dari Internet saat Anda tidak menggunakannya. DSL dan modem kabel memungkinkan pengguna untuk online setiap saat, tetapi kenyamanan ini disertai dengan risiko. Kemungkinan penyerang atau virus yang memindai jaringan untuk komputer yang tersedia akan menargetkan komputer Anda menjadi jauh lebih tinggi jika komputer Anda selalu terhubung.
- Evaluasi pengaturan keamanan Anda. Penting untuk memeriksa pengaturan komputer Anda, terutama pengaturan keamanan, dan memilih opsi yang memenuhi kebutuhan Anda tanpa meningkatkan risiko. Banyak, tetapi tidak semua penyedia Internet menawarkan perangkat lunak keamanan gratis. Jika Anda tidak menerima perangkat lunak gratis, Anda harus mempertimbangkan untuk membeli produk komersial yang mencakup pemindaian virus, firewall, dan pemblokir pop-up. Anda juga harus mengetahui pengaturan cookie Internet Anda. Cookie adalah potongan data pendek yang digunakan oleh server web untuk mengidentifikasi pengguna. Beberapa cookie berguna untuk menyimpan gambar dan data dari situs web yang sering Anda kunjungi, tetapi cookie lainnya berbahaya dan mengumpulkan informasi tentang Anda. Anda harus memutuskan seberapa besar risiko dari cookie yang dapat Anda terima. Terakhir, jika Anda menginstal tambalan atau versi baru perangkat lunak, atau jika Anda mendengar sesuatu yang mungkin memengaruhi pengaturan Anda, evaluasi kembali pengaturan Anda untuk memastikannya masih sesuai.
- Cari pernyataan atau segel kebijakan privasi yang menunjukkan bahwa situs mematuhi standar privasi. Luangkan waktu untuk membaca bagaimana privasi Anda dilindungi.
- Cari sinyal bahwa Anda menggunakan halaman web yang aman. Situs yang aman mengenkripsi atau mengacak informasi pribadi sehingga tidak dapat dengan mudah disadap. Sinyal termasuk pemberitahuan layar yang mengatakan Anda berada di situs

aman, kunci tertutup atau kunci tidak terputus di sudut bawah layar Anda, atau huruf pertama dari alamat Internet yang Anda lihat berubah dari "http" menjadi "https."

8.3 MASALAH PRIVASI ONLINE DAN PENGAWASAN ONLINE

Pengawasan dan Akses Online:

ITA juga memungkinkan campur tangan privasi pengguna secara online dengan mendefinisikan standar akses yang luas ke lembaga penegak hukum dan keamanan, dan memberi pemerintah kekuatan untuk menentukan alat apa yang dapat digunakan individu untuk melindungi privasi mereka. Hal ini paling jelas ditunjukkan oleh ketentuan yang mengizinkan intersepsi, pemantauan, dan dekripsi komunikasi digital menyediakan pengumpulan dan pemantauan data lalu lintas dan memungkinkan pemerintah untuk menetapkan standar enkripsi nasional. Secara khusus, struktur ketentuan ini dan kurangnya perlindungan yang dimasukkan, berfungsi sebagai pengenceran terhadap privasi pengguna. Misalnya, meskipun ketentuan ini menciptakan kerangka kerja untuk penyadapan, mereka kehilangan sejumlah perlindungan dan praktik yang diakui secara internasional, seperti pemberitahuan kepada individu, pengawasan yudisial, dan persyaratan transparansi.

Lebih lanjut, ketentuan tersebut menempatkan kewajiban keamanan dan teknis yang ekstensif pada penyedia layanan – karena ketentuan tersebut diharuskan untuk memperluas semua fasilitas yang diperlukan bagi badan keamanan untuk intersepsi dan dekripsi, dan membuat penyedia layanan bertanggung jawab atas hukuman penjara hingga tujuh tahun karena ketidakpatuhan. Ini menciptakan lingkungan di mana kecil kemungkinan penyedia layanan akan menentang permintaan akses atau intersepsi apa pun dari penegak hukum. Intersepsi juga diatur melalui ketentuan dan aturan di bawah Indian Telegraph Act 1885 dan lisensi ISP dan UAS berikutnya.

Lingkup Pengawasan dan Akses:

Sejauh mana Pemerintah India secara sah menyadap komunikasi tidak sepenuhnya jelas, tetapi pada tahun 2011 item berita mengutip bahwa pada bulan Juli 8.736 telepon dan akun email berada di bawah pengawasan yang sah.

Meskipun jumlah ini mewakili intersepsi resmi, ada sejumlah contoh intersepsi tidak sah yang juga terjadi. Sebagai contoh, pada tahun 2013 ditemukan bahwa di Himachel Pradesh 1371 telepon disadap berdasarkan persetujuan lisan, sedangkan Kementerian Dalam Negeri hanya mengizinkan penyadapan 170. Ini menunjukkan bahwa ada contoh ketika perlindungan yang ada untuk penyadapan dan pengawasan dirusak dan disorot tantangan penegakan bahkan untuk perlindungan yang ada.

Menunjukkan ketegangan antara hak atas privasi dan akses pemerintah ke komunikasi, dan pada saat yang sama menyoroti masalah yurisdiksi adalah kebuntuan antara RIM/BlackBerry dan Pemerintah India. Selama beberapa tahun, Pemerintah India telah meminta RIM untuk menyediakan akses ke lalu lintas komunikasi perusahaan, baik BIS dan BES, karena badan keamanan India tidak dapat mendekripsi data tersebut. Solusi yang diusulkan Pemerintah India meliputi: RIM menyediakan kunci dekripsi kepada pemerintah, RIM membangun server lokal, ISP lokal dan perusahaan telekomunikasi mengembangkan solusi pemantauan lokal. Pada 2012, RIM akhirnya mendirikan server di Mumbai dan pada 2013 memberikan solusi intersepsi sah yang memuaskan Pemerintah India.

Penerapan Sistem Pemantauan Pusat oleh Pemerintah India adalah contoh lain dari Pemerintah yang mencari akses komunikasi yang lebih besar.

Sistem ini akan memungkinkan badan keamanan untuk melewati penyedia layanan dan secara langsung mencegat komunikasi. Tidak jelas apakah sistem tersebut hanya akan menyediakan intersepsi komunikasi telepon atau apakah sistem tersebut juga akan memungkinkan intersepsi komunikasi digital dan lalu lintas internet. Juga tidak jelas check and balances apa yang ada dalam sistem. Dengan menghapus penyedia layanan dari persamaan, pemerintah tidak hanya menghilangkan cek potensial, karena penyedia layanan dapat menolak permintaan yang tidak sah, tetapi juga menghilangkan kemungkinan bagi perusahaan untuk transparan tentang permintaan intersepsi yang mereka patuhi.

8.4 MASALAH KEBIJAKAN PRIVASI

Meskipun beberapa situs Web masih kekurangan kebijakan privasi yang diposting, semakin banyak situs yang memilikinya — meskipun mereka mungkin memerlukan beberapa pencarian untuk menemukannya. Setelah ditemukan, penting untuk membaca kebijakan dengan cermat, sehingga Anda dapat yakin bahwa Anda setuju dengannya. Beberapa kebijakan privasi mungkin tidak jelas, ambigu, sulit dipahami, atau mungkin merujuk pada hubungan yang tidak ditentukan dengan perusahaan yang tidak ditentukan. Anda mungkin juga perlu membaca "Syarat dan Ketentuan," Perjanjian Pengguna/Pelanggan/Layanan, atau yang setara, karena ini dapat mengubah kebijakan privasi. Misalnya, kebijakan privasi di satu situs Web menyatakan dengan jelas bahwa tidak ada informasi yang akan dibagikan tanpa izin pengguna, tetapi perjanjian pelanggan yang menyertainya menyatakan bahwa dengan berlangganan, pengguna secara otomatis memberikan izin untuk informasi mereka dibagikan Terlepas dari kata-kata privasi saat ini kebijakan atau pemberitahuan hukum lainnya, frasa "perubahan dapat dilakukan kapan saja" relatif umum dalam perjanjian ini.

Bahkan, kesepakatan sering menyatakan bahwa perubahan ini dapat dilakukan tanpa pemberitahuan. Pengguna harus secara teratur memeriksa pemberitahuan untuk pembaruan atau perubahan. Berikut adalah salah satu contoh dari Amazon.com, meskipun perusahaan menambahkan klausa "opt-out": "Amazon.com tidak menjual, memperdagangkan, atau menyewakan informasi pribadi Anda kepada orang lain. Armand Prieditis, CEO of Unconventional Wisdom, telah mengembangkan sejumlah pertanyaan untuk menilai kebijakan privasi, termasuk berikut ini: Apakah kebijakan tersebut menonjol dan mudah diakses? Apakah jelas? Apakah singkat? Informasi apa yang dikumpulkan? Apakah tersedia pilihan untuk tidak ikut? Apakah ada ketentuan yang harus dibuat pengguna? perubahan, pembaruan, atau penghapusan data pribadi mereka Apakah ada kontak yang diberikan di perusahaan untuk pertanyaan yang berkaitan dengan praktik privasi mereka?

Dalam upaya untuk mengurangi kebutuhan untuk membaca beberapa, sering membingungkan, kebijakan privasi, The World Wide Web Consortium [http://W3c.org] sedang mengembangkan Platform untuk Preferensi Privasi (P3P) [http://www.w3. org/P3P/]. Karena keluar pada musim panas tahun 2000, P3P akan memungkinkan pengguna untuk memilih preferensi mereka sendiri mengenai jenis dan jumlah informasi yang ingin mereka berikan. Pengguna akan diperingatkan saat menjelajahi situs yang memiliki kebijakan privasi yang melampaui batas privasi yang telah ditentukan sebelumnya. Pada tulisan ini Microsoft

baru saja berjanji untuk menyediakan alat Internet gratis untuk P3P pada musim gugur tahun 2000. Namun, P3P adalah subyek dari beberapa kontroversi. Beberapa kritikus merasa bahwa insentif bagi situs Web untuk mendaftar dalam program ini tidak cukup. Presiden pemusnah sampah Jason Catlett mengatakan bahwa adopsi yang luas masih berlangsung bertahun-tahun lagi (The New York Times, 4/7/2000). Catlett mengatakan bahwa perusahaan menggunakan P3P sebagai "alasan untuk digunakan dalam lobi mereka terhadap hak privasi yang dapat ditegakkan bagi konsumen Amerika: Dalih untuk Penundaan Privasi" [http://www.cfp2000.org/papers/catlett.pdf]. Bahkan jika Anda menyetujui kebijakan privasi situs, jaminan apa yang Anda miliki bahwa situs tersebut akan benar-benar mematuhi kebijakan yang diposting? Sebuah studi baru-baru ini oleh California HealthCare Foundation menuduh bahwa sejumlah situs Web perawatan kesehatan berbagi informasi kesehatan konsumen pribadi dengan situs lain yang melanggar kebijakan privasinya sendiri. Komisi Perdagangan Federal telah diminta untuk meninjau tuduhan ini.

Segel Privasi — Tata graha yang Baik? Sejumlah segel privasi online telah dibuat dalam upaya untuk meyakinkan konsumen tentang ketentuan kebijakan privasi yang sering membingungkan. Segel ini termasuk TRUSTe, CPA WebTrust, BBBOnline, dan SecureAssure. Semua segel ini menetapkan standar yang harus dipenuhi oleh situs yang berpartisipasi.

Kritikus menuduh bahwa ada konflik kepentingan yang melekat dengan program sertifikat yang disubsidi oleh biaya dari situs yang berpartisipasi. Mereka juga mendakwa mereka dengan kurangnya tindakan penegakan hukum. Program jarang mencabut segel, bahkan untuk pelanggaran yang mencolok. TRUSTe secara khusus disebut sebagai upaya oleh industri untuk menghindari pengawasan pemerintah, dan bahwa "...membuktikan bahwa pengaturan mandiri industri tentang privasi tidak akan berhasil" (Industry Standard, 20 Maret 2000, hlm. 168). Sertifikasi pihak ketiga yang independen bisa sangat berguna dalam meningkatkan kepercayaan konsumen, terutama mengenai isu-isu sensitif. Salah satu aplikasi yang sangat berguna mungkin terletak pada jaminan keamanan situs terhadap serangan peretas, karena dapat dimengerti bahwa perusahaan enggan untuk merinci pengaturan keamanan secara terbuka di situs Web mereka.

8.5 PEKERJAAN OECD TENTANG PRIVASI

Selama beberapa dekade, OECD telah memainkan peran penting dalam mempromosikan penghormatan terhadap privasi sebagai nilai fundamental dan syarat untuk arus bebas data pribadi lintas batas. Landasan kerja OECD tentang privasi adalah Pedoman yang baru direvisi tentang Perlindungan Privasi dan Arus Data Pribadi Lintas Batas (2013). Komponen kunci lain dari pekerjaan di bidang ini bertujuan untuk meningkatkan kerjasama lintas batas di antara otoritas penegak hukum privasi. Karya ini menghasilkan Rekomendasi OECD tentang Kerjasama Lintas Batas dalam Penegakan Hukum Melindungi Privasi pada tahun 2007 dan mengilhami pembentukan Jaringan Penegakan Privasi Global, yang didukung oleh OECD. Proyek lain telah memeriksa pemberitahuan privasi dan mempertimbangkan privasi dalam konteks masalah horizontal seperti identifikasi frekuensi radio (RFID), manajemen identitas digital, dan melihat metrik untuk menginformasikan pembuatan kebijakan di bidang ini. Peran penting privasi juga dibahas dalam Rekomendasi OECD tentang Prinsip untuk Pembuatan Kebijakan Internet (2011) dan Deklarasi Menteri Seoul tentang Masa Depan

Ekonomi Internet (2008). Pekerjaan saat ini sedang memeriksa masalah terkait privasi yang diangkat oleh penggunaan data dan analitik skala besar. Sebuah meja bundar ahli diadakan untuk mendukung pekerjaan itu pada bulan Maret 2014. Ini adalah bagian dari proyek yang lebih luas tentang inovasi dan pertumbuhan berbasis data, yang telah menghasilkan laporan awal yang mengidentifikasi masalah-masalah utama.

Pedoman Privasi OECD 2013 Revisi yang disepakati pada tahun 2013 meliputi:

- Rekomendasi Dewan OECD tentang Pedoman
- mengatur Perlindungan Privasi dan Arus Lintas Batas Data Pribadi (Juli 2013); dan
- Nota penjelasan baru yang memberikan konteks dan alasan untuk revisi Juli 2013.

Pedoman baru ini merupakan pembaruan pertama dari versi asli tahun 1980 yang berfungsi sebagai seperangkat prinsip privasi pertama yang disepakati secara internasional. Dua tema dijalankan melalui Pedoman yang diperbarui. Pertama, fokus pada implementasi praktis perlindungan privasi melalui pendekatan yang didasarkan pada manajemen risiko. Kedua adalah perlunya upaya yang lebih besar untuk mengatasi dimensi privasi global melalui peningkatan interoperabilitas. Sejumlah konsep baru diperkenalkan, termasuk:

- Strategi privasi nasional. Sementara undang-undang yang efektif sangat penting, kepentingan strategis privasi saat ini juga membutuhkan strategi nasional multifaset yang dikoordinasikan di tingkat pemerintahan tertinggi.
- Program manajemen privasi. Ini berfungsi sebagai mekanisme operasional inti di mana organisasi menerapkan perlindungan privasi.
- Pemberitahuan pelanggaran keamanan data. Ketentuan ini mencakup pemberitahuan kepada otoritas dan pemberitahuan kepada individu yang terkena dampak pelanggaran keamanan yang memengaruhi data pribadi.

Revisi lainnya memodernisasi pendekatan OECD terhadap aliran data lintas batas, merinci elemen kunci dari apa artinya menjadi organisasi yang akuntabel, dan memperkuat penegakan privasi. Sebagai langkah dalam proses yang berkelanjutan, revisi ini meninggalkan "Prinsip-Prinsip Dasar" asli dari Pedoman. Pekerjaan yang sedang berlangsung oleh OECD tentang perlindungan privasi dalam ekonomi berbasis data akan memberikan peluang lebih lanjut untuk memastikan bahwa kerangka kerja privasinya disesuaikan dengan baik untuk tantangan saat ini.

Proses untuk merevisi Pedoman dipimpin oleh OECD Working Party on Information Security and Privacy (WPISP) bekerja dari kerangka acuan yang dirilis pada konferensi OECD tentang interoperabilitas global di Mexico City pada November 2011. Pekerjaan persiapan untuk revisi 2013 dilakukan di konteks peringatan 30 tahun Pedoman asli, yang ditandai dengan serangkaian konferensi dan makalah. Sesuai dengan kerangka acuan, WPISP mengumpulkan kelompok ahli multi-stakeholder dari pemerintah, otoritas penegakan privasi, akademisi, bisnis, masyarakat sipil dan komunitas teknis Internet. Kelompok ahli ini diketuai oleh Jennifer Stoddart, Komisaris Privasi Kanada. Omer Tene, konsultan OECD, menjabat sebagai pelapor. Atas dasar kerja kelompok ahli, revisi yang diusulkan dikembangkan oleh WPISP dan disetujui oleh Komite Kebijakan Informasi, Komputer dan Komunikasi (ICCP), sebelum adopsi akhir oleh Dewan OECD.

8.6 PERLINDUNGAN KEBOCORAN DATA (DLP)

Melindungi kebocoran data untuk organisasi mana pun telah menjadi perhatian utama di dunia saat ini yang dengan cepat meningkatkan kebutuhan akan solusi DLP di pasar. Namun, istilah DLP sendiri digunakan dengan cara yang berbeda oleh vendor yang berbeda. Kami di NII membantu Anda mengungkap jargon dan memilih solusi DLP yang tepat untuk organisasi Anda. Pada saat yang sama, hanya pengadaan dan penerapan solusi DLP bukanlah jawaban yang lengkap. Solusi DLP adalah teknologi yang sangat terlibat dan memiliki siklus implementasi yang intens. Jadi implementasi DLP yang sukses memerlukan perencanaan, sumber daya, konfigurasi, manajemen, dan pemantauan yang tepat untuk membantunya benar-benar melindungi kebocoran data.

Bagaimana cara kerja DLP?

Berikut ini adalah berbagai metode bagaimana perlindungan kebocoran data membantu organisasi Anda untuk melindungi informasi berharga atau sensitif Anda yang sedang transit, diam, atau sedang digunakan.

- DLP memberikan solusi yang kuat untuk melindungi data dalam transit [tindakan jaringan] dengan mengendus lalu lintas jaringan email, pesan obrolan, dll untuk menemukan konten yang dikirim melalui saluran komunikasi.
- Ini juga memberikan solusi untuk melindungi data saat istirahat dengan memindai konten area penyimpanan seperti drive USB, hard drive, dll dan menemukan konten darinya. Ini juga disebut sebagai Penemuan Konten.
- Ini juga memberikan solusi untuk melindungi data yang digunakan [tindakan titik akhir] yaitu, melindungi data yang sedang digunakan oleh pengguna misalnya jika pengguna telah menghubungkan drive USB ke komputer.

Sebagian besar solusi DLP melakukan ini dalam kombinasi berikut:

1. Ekspresi Reguler Berbasis Aturan
2. Sidik Jari Basis Data
3. Pencocokan File yang Tepat
4. Pencocokan Dokumen Sebagian
5. Analisis Statistik
6. Konseptual/Leksikon
7. Kategori

8.7 ENKRIPSI PESAN

Terkadang Anda menginginkan perlindungan tambahan untuk komunikasi email Anda agar tidak terlihat oleh mata yang tidak diinginkan. Mengenkripsi pesan email di Microsoft Office Outlook 2007 melindungi privasi pesan dengan mengubahnya dari teks biasa (yang dapat dibaca) menjadi teks sandi (diacak). Hanya penerima yang memiliki kunci pribadi yang cocok dengan kunci publik yang digunakan untuk mengenkripsi pesan yang dapat menguraikan pesan untuk dibaca. Setiap penerima tanpa kunci pribadi yang sesuai hanya akan melihat teks yang kacau.

Ini adalah proses terpisah dari menandatangani pesan secara digital.

- Mengirim dan melihat pesan email terenkripsi memerlukan pengirim dan penerima untuk berbagi ID digital mereka, atau sertifikat kunci publik. Ini berarti Anda dan

penerima masing-masing harus saling mengirim pesan yang ditandatangani secara digital, yang memungkinkan Anda menambahkan sertifikat orang lain ke Kontak Anda. Setelah kedua belah pihak memiliki sertifikat bersama, mengirim dan melihat pesan email terenkripsi di antara mereka sama seperti dengan pesan email lainnya. Anda dapat mempelajari tentang ID digital di sini dan mempelajari cara mendapatkan dan menukar ID digital di sini.

- Jika Anda mengirim pesan terenkripsi ke penerima yang pengaturan emailnya tidak mendukung enkripsi, Outlook akan memberi tahu Anda dan menawarkan opsi untuk mengirim pesan dalam format tidak terenkripsi.
- Proses ini juga mengenkripsi semua lampiran yang dikirim dengan pesan terenkripsi.

8.8 ENKRIPSI UJUNG KE UJUNG

Enkripsi "end-to-end" berarti data yang keluar dari browser Anda akan dienkripsi sampai penerima pesan yang dituju mendekripsinya, dan pesan terenkripsi serupa yang dikirimkan kepada Anda akan tetap seperti itu sampai Anda mendekripsinya di browser Anda. Meskipun alat enkripsi ujung ke ujung seperti PGP dan GnuPG telah ada sejak lama, alat ini membutuhkan banyak pengetahuan teknis dan upaya manual untuk digunakan. Untuk membantu membuat enkripsi semacam ini sedikit lebih mudah, kami merilis kode untuk ekstensi Chrome baru yang menggunakan OpenPGP, standar terbuka yang didukung oleh banyak alat enkripsi yang ada.

Namun, Anda belum akan menemukan ekstensi End-to-End di Toko Web Chrome; kami hanya membagikan kode hari ini sehingga komunitas dapat menguji dan mengevaluasinya, membantu kami memastikan bahwa kode tersebut seaman yang diperlukan sebelum orang-orang mulai mengandalkannya. Setelah kami merasa bahwa ekstensi siap untuk primetime, kami akan membuatnya tersedia di Toko Web Chrome, dan siapa pun akan dapat menggunakannya untuk mengirim dan menerima email terenkripsi ujung ke ujung melalui penyedia email berbasis web yang ada . Kami menyadari bahwa enkripsi semacam ini mungkin hanya akan digunakan untuk pesan yang sangat sensitif atau oleh mereka yang membutuhkan perlindungan tambahan. Namun kami berharap ekstensi End-to-End akan mempercepat dan mempermudah orang-orang untuk mendapatkan lapisan keamanan ekstra jika mereka membutuhkannya.

8.9 KEBIJAKAN KEAMANAN CYBER NASIONAL PEMERINTAH INDIA, 2013

Pada tanggal 2 Juli 2013, pemerintah India merilis Kebijakan Keamanan Siber Nasional 2013 yang ambisius. Perkembangan kebijakan tersebut didorong oleh berbagai: faktor, termasuk pertumbuhan industri teknologi informasi India, peningkatan jumlah serangan dunia maya dan "rencana ambisius negara untuk transformasi sosial yang cepat." Kebijakan tersebut menetapkan 14 tujuan beragam yang berkisar dari meningkatkan perlindungan infrastruktur penting India, untuk membantu penyelidikan dan penuntutan kejahatan dunia maya, hingga mengembangkan 500.000 profesional keamanan dunia maya yang terampil selama lima tahun ke depan.

Untuk mencapai tujuan ini, kebijakan tersebut merinci banyak item tindakan untuk pemerintah India, termasuk:

- Menunjuk badan nasional untuk mengoordinasikan semua masalah keamanan siber;
- Mendorong semua organisasi swasta dan publik untuk menunjuk Chief Information Security Officer yang bertanggung jawab atas keamanan cyber;
- Mengembangkan kerangka hukum yang dinamis untuk mengatasi tantangan keamanan dunia maya di bidang komputasi awan, komputasi seluler, dan media sosial;
- Mengoperasikan Pusat Perlindungan Infrastruktur Informasi Kritis Nasional;
- Mempromosikan penelitian dan pengembangan keamanan siber;
- Meningkatkan kerja sama global dalam memerangi ancaman keamanan siber;
- Membina program pendidikan dan pelatihan di bidang keamanan siber; dan
- Membangun kemitraan publik dan swasta untuk menentukan praktik terbaik dalam keamanan siber.

Dalam mengumumkan kebijakan tersebut, Menteri Komunikasi dan Informatika India Kapil Sibal (Mantan Menteri) mencatat bahwa operasionalisasi kebijakan tersebut akan menjadi tantangan yang pada akhirnya diperlukan untuk "memastikan tidak ada gangguan yang akan mengganggu stabilitas ekonomi."

DSCI (Dewan Keamanan Data India) mulai berfungsi sebagai perusahaan independen dengan Dewannya sendiri, dan tim inti kecil yang terdiri dari pakar teknis, dipandu oleh Komite Pengarah pada Agustus 2008. Panduan mereka memungkinkan DSCI menentukan misinya, yang pada gilirannya membantunya menyusun Rencana Kerja, dengan pendekatan praktis untuk melibatkan industri melalui Program Agregasi Konten kami. Program ini terdiri dari pemetaan peraturan ke dalam kontrol, dan menurunkan praktik terbaik dari yang sama. Praktik Terbaik untuk Keamanan Data dan Privasi Data telah dikembangkan menggunakan pengalaman standar keamanan ISO 27001, dan Prinsip Privasi OECD, dan penerapan kerangka kerja pemerintah seperti FISMA di AS; serta rekomendasi para analis dan pedoman taktis yang muncul selama beberapa tahun terakhir. Praktik terbaik akan memungkinkan penyedia layanan di India untuk tidak hanya mematuhi persyaratan peraturan, tetapi juga membuatnya benar-benar aman.

DSCI terlibat dengan pemangku kepentingan di AS, Inggris, Uni Eropa, dan beberapa negara lain untuk membuat mereka sadar akan penekanan pada praktik keamanan dan privasi oleh industri TI/BPO India. Ini melalui presentasi, dan diskusi dengan, otoritas perlindungan data dan klien di sejumlah seminar dan lokakarya. DSCI terlibat dengan industri TI/BPO sepanjang tahun melalui sejumlah seminar dan lokakarya kesadaran keamanan, dan tentang perlunya praktik dan standar terbaik untuk meningkatkan kepercayaan mereka. Industri telah menanggapi dengan baik Pendekatan Perlindungan Data DSCI berdasarkan praktik terbaik, dan tujuannya untuk menjadi organisasi yang mengatur diri sendiri. Untuk melindungi privasi informasi pribadi dari penggunaan, pengungkapan, modifikasi, atau penyalahgunaan yang tidak sah, DSCI mengkonseptualisasikan pendekatannya terhadap privasi di

DSCI Privacy Framework (DPF yang didasarkan pada praktik dan kerangka kerja terbaik privasi global. Kerangka ini dirilis pada bulan Desember 2010. Untuk menilai implementasi privasi dalam suatu organisasi, DSCI Assessment Framework for Privacy (DAF-P) dirilis pada bulan Desember, 2012. Ini terdiri dari dua bagian, dengan masing-masing berfokus pada aspek penerapan privasi yang berbeda – satu berfokus pada Penilaian Kompetensi Organisasi dalam Privasi berdasarkan area praktik yang ditentukan dalam DPF sementara yang lain – Penilaian

berdasarkan Prinsip Privasi, berfokus pada penerapan prinsip privasi global Bagian pertama didasarkan pada sembilan bidang praktik yang terdaftar di bawah DPF dan kuesioner penilaian dirancang untuk membantu organisasi menilai dan mematangkan program privasi mereka.

Kuesioner didasarkan pada praktik yang didefinisikan dalam DPF, dengan parameter panduan sugestif untuk membantu penilai saat melakukan penilaian.Penilaian dapat dilakukan dalam salah satu mode: Penilaian Diri atau Penilaian Eksternal nt. Asesmen eksternal melalui auditor empaneled DSCI dapat membantu organisasi mencapai Sertifikasi DSCI. Bagian kedua dimaksudkan untuk membantu organisasi menilai dan meningkatkan kedewasaan dalam penerapan prinsip privasi global di semua proses organisasi yang berhubungan dengan informasi pribadi dan dalam proses mengoptimalkan upaya mereka sambil menerapkan prinsip privasi di seluruh operasi global. DSCI telah merancang program pelatihan bagi penilai potensial untuk menilai penerapan privasi dalam organisasi yang memenuhi persyaratan yang ditetapkan dalam DPF.

Tujuan: Untuk melengkapi penilai potensial dengan pengetahuan dan alat yang diperlukan untuk menilai implementasi privasi organisasi sesuai dengan DSCI Assessment Framework for Privacy (DAF-P) dan DSCI Privacy Framework. Program pelatihan bermaksud untuk menjelaskan maksud di balik setiap praktik yang didefinisikan di bawah sembilan area praktik (DPF), untuk membantu penilai memahami, menganalisis, menyelidiki, dan menghargai berbagai aspek penerapan privasi dalam organisasi. Program pelatihan bertujuan untuk menyediakan platform bersama bagi penilai potensial dari berbagai organisasi untuk memiliki pemahaman dan harapan yang sama untuk implementasi privasi. Program ini juga akan membantu organisasi yang menginginkan sertifikasi DSCI; lebih memahami harapan implementasi privasi, dan persyaratan untuk sertifikasi DSCI.

8.10 PANDUAN UNTUK KAFE CYBER DI INDIA

Pada tahun 2011 Pedoman Aturan Cyber Cafe diberitahukan di bawah Undang-Undang Teknologi Informasi. Aturan ini, antara lain, mengharuskan Warnet untuk menyimpan rincian berikut untuk setiap pengguna untuk jangka waktu satu tahun: rincian identifikasi, nama, alamat, nomor kontak, jenis kelamin, tanggal, identifikasi terminal komputer, lama waktu, dan lama keluar waktu. Rincian ini harus diserahkan ke agensi yang sama seperti yang diarahkan, setiap bulan. Warnet juga harus menyimpan riwayat situs web yang diakses dan log dari server proxy yang dipasang di warnet untuk jangka waktu satu tahun. Selanjutnya, Cyber Cafe harus memastikan bahwa partisi antar bilik tidak melebihi ketinggian empat setengah kaki dari lantai. Terakhir, pemilik warnet wajib memberikan setiap dokumen, daftar, dan informasi terkait kepada petugas yang diberi wewenang oleh lembaga pendaftaran sesuai permintaan. Akibatnya, persyaratan identifikasi dan penyimpanan aturan ini berdampak pada privasi dan kebebasan berekspresi, karena pengguna warnet tidak dapat menggunakan fasilitas secara anonim dan semua informasi mereka, termasuk riwayat browser, disimpan secara a-priori.

Ketentuan pengungkapan dalam aturan ini juga berdampak pada privasi dan menunjukkan penurunan standar akses untuk penegakan hukum kepada pengguna komunikasi internet karena ketentuan tersebut tidak mendefinisikan:

- Proses otorisasi yang diikuti oleh agen pendaftaran untuk memberi wewenang kepada individu untuk melakukan inspeksi.

- Keadaan di mana pemeriksaan Cyber Cafe oleh petugas yang berwenang diperlukan dan diperbolehkan.
- Proses dimana informasi dapat diminta, dan sebaliknya secara samar-samar mengharuskan pemilik warnet untuk mengungkapkan informasi "sesuai permintaan".

8.11 RINGKASAN

Tidak ada konsensus di seluruh dunia tentang privasi online dan masalah sekuritas karena beberapa kepentingan industri. Dalam unit ini konsep risiko online, masalah privasi online dan pengawasan online, masalah kebijakan privasi, OECD bekerja pada privasi, melindungi data dalam perjalanan, enkripsi pesan, Enkripsi End-to-End, Pemerintah India dan Kebijakan Keamanan Cyber, 2013 dan Pedoman untuk Cyber Security Café di India dibahas panjang lebar untuk memahami masalah privasi dan sekuritas online di India dan di seluruh dunia.

8.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Penulis)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)

- Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

8.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut yang benar atau salah:
   a Pertumbuhan penggunaan internet yang menakjubkan di beberapa negara juga meningkatkan kekhawatiran tentang privasi.
   b Menggunakan perangkat pelacak yang dikenal sebagai "cookies", perusahaan dapat melacak pembelian dan mengumpulkan data pribadi.
   c Keamanan dunia maya, phishing, worm, firewall, Trojan horse, peretas, dan virus tampaknya menjadi berita setiap hari.
   d Beberapa situs web masih kekurangan kebijakan privasi yang diposting.
   e Selama beberapa dekade, OECD telah memainkan peran penting dalam mempromosikan penghormatan terhadap privasi sebagai nilai fundamental dan kondisi untuk arus bebas data pribadi lintas batas.

B. Isi Bagian yang Kosong:
   I. Sebuah .....program adalah perangkat lunak yang mengklaim melakukan satu hal sementara, sebenarnya melakukan sesuatu yang berbeda di belakang layar.
   II. Penyadapan juga diatur melalui ketentuan dan aturan di bawah.....
   III. Landasan kerja OECD tentang privasi adalah yang baru direvisi.....
   IV. DLP berarti.....
   V. DSCI artinya.....

8.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Kuda Troya
2. Undang-Undang Telegraf India, 1885
3. Pedoman perlindungan privasi dan arus transformator data pribadi
4. Perlindungan Kebocoran Data
5. Dewan Keamanan Data India

8.15 PERTANYAAN TERMINAL

1. Apa itu risiko online?
2. Diskusikan privasi online.
3. Apa pekerjaan OECD tentang privasi?

4. Diskusikan Pemerintah India dan Kebijakan Keamanan Cyber, 2013.
5. Apa pedoman untuk warnet keamanan siber di India?

BAB 9
SEKURITAS INTERNET: KONSEP, ALAT DAN ISU TERKAIT

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami masalah dan hal-hal yang terkait dengan Keamanan Internal
- Memahami ancaman dan tantangan jika terjadi gangguan di Keamanan Internal
- Memahami masalah teknis dan hukum terkait Keamanan Internal

9.1 PENGANTAR

Sifat Internet yang terbuka membuatnya penting bagi bisnis untuk memperhatikan keamanan jaringan mereka. Ketika perusahaan memindahkan lebih banyak fungsi bisnis mereka ke jaringan publik, mereka perlu mengambil tindakan pencegahan untuk memastikan bahwa data tidak dapat dikompromikan dan bahwa data tersebut tidak dapat diakses oleh siapa pun yang tidak berwenang untuk melihatnya. Akses jaringan yang tidak sah oleh peretas luar atau karyawan yang tidak puas dapat menyebabkan kerusakan atau kehancuran pada data kepemilikan, berdampak negatif pada produktivitas perusahaan, dan menghambat kemampuan untuk bersaing. Institut Keamanan Komputer melaporkan dalam Survei Kejahatan dan Keamanan Komputer CSI 2010/2011 (tersedia di http://gocsi.com/survey) bahwa pada hari rata-rata, 41,1 persen responden menangani setidaknya satu insiden keamanan. Akses jaringan yang tidak sah juga dapat merusak hubungan dengan pelanggan dan mitra bisnis, yang mungkin mempertanyakan kemampuan perusahaan untuk melindungi informasi rahasianya. Definisi "lokasi data" sedang dikaburkan oleh layanan komputasi kaleng dan tren layanan lainnya. Individu dan perusahaan mendapat manfaat dari penyebaran layanan yang elastis di cloud, tersedia setiap saat dari perangkat apa pun, tetapi perubahan dramatis dalam industri layanan bisnis ini memperburuk risiko dalam melindungi data dan entitas yang menggunakannya (individu, bisnis, pemerintah, dan segera). Kebijakan dan arsitektur keamanan memerlukan prinsip yang baik dan pendekatan siklus hidup, termasuk apakah data ada di server farm, seluler di laptop karyawan, atau disimpan di cloud.

9.2 KEAMANAN INTERNET: SIAPA YANG HARUS ANDA PERCAYAI?

Dalam artikel terbaru Forbe "Keamanan Internet: Siapa yang Harus Anda Percayai", subjek mengetahui siapa yang harus dipercaya secara online ketika dihadapkan dengan tantangan berkelanjutan untuk dapat mengotentikasi entitas yang sah secara online. Dalam artikel ini, kita mempelajari lebih lanjut tentang bagaimana "...keamanan internet adalah tentang kepercayaan dari jauh" serta apa yang dilakukan pemerintah AS, khususnya 'Online Trust Alliance' (OTA) untuk melindungi warganya dari penipuan dan penipu online. OTA mewakili lebih dari 100 perusahaan dan organisasi yang "...mencerminkan ekosistem internet yang luas." Gabungan, mereka telah menjalin hubungan integral dengan keamanan utama dan pengembang virus, Microsoft, situs jejaring sosial dan sistem pembayaran online seperti Paypal. Pekan lalu di kantor Kejaksaan Agung New York, mereka bertemu dengan FBI untuk membahas kejahatan dunia maya global. OTA bertujuan untuk "meningkatkan kepercayaan

online" sambil mendorong vitalitas dan inovasi di web. Untuk bisnis, upaya ini "...diterjemahkan ke dalam keamanan, privasi, reputasi dan kewajiban dan uang."

9.3 ETIKA PENELITIAN INTERNET

Etika penelitian internet adalah subdisiplin yang cocok dengan banyak disiplin ilmu, mulai dari ilmu sosial, seni dan humaniora, kedokteran/biomedis, dan ilmu keras. Kerangka kerja etika yang ada, termasuk konsekuensialisme, utilitarianisme, deontologi, etika kebajikan, dan etika feminis telah berkontribusi pada cara-cara di mana masalah etika dalam penelitian Internet dipertimbangkan dan dievaluasi. Secara konseptual dan historis, etika penelitian Internet terkait dengan komputer dan etika informasi dan mencakup masalah etika seperti privasi dan kerahasiaan data, integritas data, masalah kekayaan intelektual, dan standar profesional. Sepanjang evolusi Internet, ada perdebatan apakah ada dilema etika baru yang muncul, atau apakah dilema yang ada konsisten di seluruh penelitian atau terlepas dari pengaruh teknologi (Elgesem 2002; Walther 2002; Ess & AoIR 2002). Perdebatan ini mirip dengan debat filosofis dalam etika komputer dan informasi. Misalnya, bertahun-tahun yang lalu, Moor bertanya "apa yang istimewa tentang komputer" untuk memahami apa yang unik secara etis dan pertanyaan yang sama berlaku untuk penelitian Internet (Moor 1985; Ess & AoIR 2002; King 1996).

Namun, karena Internet telah berkembang menjadi alat dan tempat yang lebih sosial dan komunikatif, masalah etika telah bergeser dari murni berbasis data menjadi lebih manusiawi terpusat. Analogi "di lapangan" atau tatap muka mungkin tidak berlaku untuk penelitian online. Misalnya, konsep taman umum telah digunakan sebagai situs di mana peneliti dapat mengamati orang lain, tetapi secara online, konsep publik dan privat jauh lebih kompleks. Dengan demikian, beberapa ahli menyarankan bahwa kekhususan etika penelitian Internet memerlukan pedoman peraturan dan/atau profesional dan disiplin baru. Untuk alasan ini, konsep kebijakan dan peraturan penelitian subyek manusia menginformasikan entri ini, bersama dengan standar disiplin, yang akan mengeksplorasi area yang berkembang dari kompleksitas etika dan metodologis, termasuk identifikasi pribadi, risiko dan bahaya reputasi, gagasan tentang ruang publik dan teks publik. , kepemilikan, dan umur panjang data yang terkait dengan penelitian Internet.

Secara khusus, kemunculan web sosial menimbulkan masalah seputar praktik perekrutan subjek atau peserta, model persetujuan berdasarkan informasi berjenjang, dan perlindungan berbagai harapan dan bentuk privasi di dunia teknologi yang tersebar dan ada di mana-mana yang terus meningkat; anonimitas dan kerahasiaan data di ruang di mana peneliti dan subjeknya mungkin tidak sepenuhnya memahami syarat dan ketentuan tempat atau alat tersebut; tantangan terhadap integritas data karena proyek penelitian dapat dialihdayakan ke mekanik atau bot; dan masalah yurisdiksi karena lebih banyak penelitian diproses, disimpan, dan disebarluaskan melalui komputasi awan atau di server lokal yang jauh, menghadirkan berbagai kompleksitas hukum mengingat perbedaan yurisdiksi dalam undang-undang data.

Akibatnya, para peneliti menggunakan Internet sebagai alat atau ruang penelitian — dan dewan etika penelitian (REB), juga dikenal sebagai dewan peninjau institusional (IRB) di Amerika Serikat atau komite etika penelitian manusia (HREC) di negara lain. seperti Australia —

telah dihadapkan dengan serangkaian pertanyaan etika baru: Kewajiban etis apa yang dimiliki peneliti untuk melindungi privasi subjek yang terlibat dalam aktivitas di ruang Internet "publik"? Bagaimana kerahasiaan atau anonimitas dijamin secara online? Bagaimana dan haruskah informed consent diperoleh secara online? Bagaimana seharusnya penelitian tentang anak di bawah umur dilakukan, dan bagaimana Anda membuktikan bahwa suatu subjek bukan anak di bawah umur? Apakah penipuan (berpura-pura menjadi seseorang yang bukan Anda, menyembunyikan informasi yang dapat diidentifikasi, dll) secara online merupakan norma atau bahaya? Bagaimana "bahaya" mungkin terjadi pada seseorang yang ada di ruang online?

9.4 MASALAH KEAMANAN INTERNET

Semua komunikasi melalui Internet menggunakan Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP memungkinkan informasi dikirim dari satu komputer ke komputer lain melalui berbagai komputer perantara dan jaringan terpisah sebelum mencapai tujuannya. Fleksibilitas TCP/IP yang luar biasa telah menyebabkan penerimaannya di seluruh dunia sebagai protokol komunikasi Internet dan intranet dasar. Pada saat yang sama, fakta bahwa TCP/IP memungkinkan informasi melewati komputer perantara memungkinkan pihak ketiga untuk mengganggu komunikasi dengan cara berikut:

- Menguping. Informasi tetap utuh, tetapi privasinya terganggu. Misalnya, seseorang dapat mempelajari nomor kartu kredit Anda, merekam percakapan sensitif, atau mencegat informasi rahasia.
- Merusak. Informasi dalam perjalanan diubah atau diganti dan kemudian dikirim ke penerima. Misalnya, seseorang dapat mengubah pesanan barang atau mengubah resume seseorang.
- Peniruan identitas. Informasi diteruskan ke orang yang menyamar sebagai penerima yang dituju. Peniruan identitas dapat mengambil dua bentuk:
- Pemalsuan. Seseorang bisa berpura-pura menjadi orang lain. Misalnya, seseorang dapat berpura-pura memiliki alamat email jdoe@example.net, atau komputer dapat mengidentifikasi dirinya sebagai situs yang disebut www.example.net padahal sebenarnya tidak. Jenis peniruan ini dikenal sebagai spoofing.
- Representasi yang salah. Seseorang atau organisasi dapat salah menggambarkan dirinya sendiri. Misalnya, situs www.example.net berpura-pura menjadi toko furnitur padahal sebenarnya hanya situs yang menerima pembayaran kartu kredit tetapi tidak pernah mengirim barang apa pun.

Biasanya, pengguna dari banyak komputer yang bekerja sama yang membentuk Internet atau jaringan lain tidak memantau atau mengganggu lalu lintas jaringan yang terus menerus melewati mesin mereka. Namun, banyak komunikasi pribadi dan bisnis yang sensitif melalui Internet memerlukan tindakan pencegahan yang mengatasi ancaman yang tercantum di atas. Untungnya, seperangkat teknik dan standar mapan yang dikenal sebagai kriptografi kunci publik membuatnya relatif mudah untuk mengambil tindakan pencegahan tersebut. Kriptografi kunci publik memfasilitasi tugas-tugas berikut:

- Enkripsi dan dekripsi memungkinkan dua pihak yang berkomunikasi untuk menyamarkan informasi yang mereka kirimkan satu sama lain. Pengirim mengenkripsi,

atau mengacak, informasi sebelum mengirimnya. Penerima mendekripsi, atau menguraikan, informasi setelah menerimanya. Saat dalam perjalanan, informasi terenkripsi tidak dapat dipahami oleh penyusup.

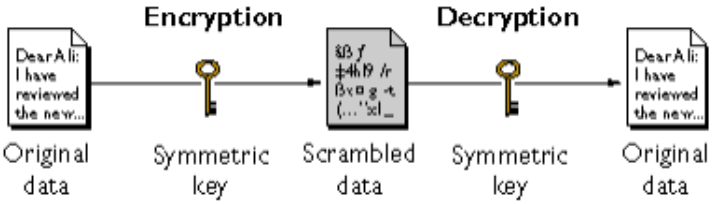
- Deteksi kerusakan memungkinkan penerima informasi untuk memverifikasi bahwa informasi tersebut tidak diubah dalam perjalanan. Setiap upaya untuk mengubah data atau mengganti pesan palsu dengan yang sah akan terdeteksi.
- Otentikasi memungkinkan penerima informasi untuk menentukan asalnya- yaitu, untuk mengkonfirmasi identitas pengirim.
- Non repudiation mencegah pengirim informasi untuk mengklaim di kemudian hari bahwa informasi tersebut tidak pernah dikirim.44

9.5 ENKRIPSI DAN DEKRIPSI

Enkripsi adalah proses mengubah informasi sehingga tidak dapat dipahami oleh siapa pun kecuali penerima yang dituju. Dekripsi adalah proses mengubah informasi terenkripsi sehingga dapat dipahami kembali. Algoritma kriptografi, juga disebut cipher, adalah fungsi matematika yang digunakan untuk enkripsi atau dekripsi. Dalam kebanyakan kasus, dua fungsi terkait digunakan, satu untuk enkripsi dan yang lainnya untuk dekripsi. Dengan sebagian besar kriptografi modern, kemampuan untuk menjaga kerahasiaan informasi terenkripsi tidak didasarkan pada algoritma kriptografi, yang dikenal luas, tetapi pada nomor yang disebut kunci yang harus digunakan dengan algoritma untuk menghasilkan hasil terenkripsi atau untuk mendekripsi informasi yang sebelumnya dienkripsi. . Dekripsi dengan kunci yang benar sederhana. Dekripsi tanpa kunci yang benar sangat sulit, dan dalam beberapa kasus tidak mungkin untuk semua tujuan praktis.

Bagian berikut memperkenalkan penggunaan kunci untuk enkripsi dan dekripsi.

- Enkripsi Kunci Simetris
- Enkripsi Kunci Publik
- Panjang Kunci dan Kekuatan Enkripsi
- Enkripsi Kunci Simetris: Dengan enkripsi kunci simetris, kunci enkripsi dapat dihitung dari kunci dekripsi dan sebaliknya. Dengan sebagian besar algoritma simetris, kunci yang sama digunakan untuk enkripsi dan dekripsi, seperti yang ditunjukkan pada Gambar 9.1.



Gambar 9.1 Enkripsi kunci otomatis

Skema yang ditunjukkan pada Gambar 9.2 memungkinkan Anda mendistribusikan kunci publik secara bebas, dan hanya Anda yang dapat membaca data yang dienkripsi menggunakan kunci ini. Secara umum, untuk mengirim terenkripsi data ke seseorang, Anda mengenkripsi data dengan kunci publik orang itu, dan orang yang menerima data terenkripsi mendekripsi dengan kunci pribadi yang sesuai.

Dibandingkan dengan enkripsi kunci simetris, enkripsi kunci publik membutuhkan lebih banyak komputasi dan oleh karena itu tidak selalu sesuai untuk data dalam jumlah besar. Namun, dimungkinkan untuk menggunakan enkripsi kunci publik untuk mengirim kunci simetris, yang kemudian dapat digunakan untuk mengenkripsi data tambahan. Ini adalah pendekatan yang digunakan oleh protokol SSL.

Seperti yang terjadi, kebalikan dari skema yang ditunjukkan pada Gambar 9.2 juga berfungsi: data yang dienkripsi dengan kunci pribadi Anda hanya dapat didekripsi dengan kunci publik Anda. Namun, ini bukan cara yang diinginkan untuk mengenkripsi data sensitif, karena ini berarti bahwa siapa pun yang memiliki kunci publik Anda, yang menurut definisi dipublikasikan, dapat mendekripsi data. Namun demikian, enkripsi kunci pribadi berguna, karena itu berarti Anda dapat menggunakan kunci pribadi Anda untuk menandatangani data dengan tanda tangan digital Anda—persyaratan penting untuk perdagangan elektronik dan aplikasi kriptografi komersial lainnya. Perangkat lunak klien seperti Firefox kemudian dapat menggunakan kunci publik Anda untuk mengonfirmasi bahwa pesan telah ditandatangani dengan kunci pribadi Anda dan bahwa pesan tersebut belum diubah sejak ditandatangani. "Tanda Tangan Digital" dan bagian selanjutnya menjelaskan cara kerja proses konfirmasi ini.
Panjang Kunci dan Kekuatan Enkripsi

Secara umum, kekuatan enkripsi terkait dengan kesulitan menemukan kunci, yang pada gilirannya tergantung pada cipher yang digunakan dan panjang kunci. Misalnya, kesulitan menemukan kunci untuk cipher RSA yang paling umum digunakan untuk enkripsi kunci publik bergantung pada kesulitan memfaktorkan bilangan besar, masalah matematika yang terkenal.

Kekuatan enkripsi sering digambarkan dalam hal ukuran kunci yang digunakan untuk melakukan enkripsi: secara umum, kunci yang lebih panjang memberikan enkripsi yang lebih kuat. Panjang kunci diukur dalam bit. Misalnya, kunci 128-bit untuk digunakan dengan cipher kunci simetris RC4 yang didukung oleh SSL memberikan perlindungan kriptografi yang jauh lebih baik daripada kunci 40-bit untuk digunakan dengan cipher yang sama. Secara kasar, enkripsi RC4 128-bit 3 x 1026 kali lebih kuat dari enkripsi RC4 40-bit. (Untuk informasi lebih lanjut tentang RC4 dan sandi lain yang digunakan dengan SSL.

Cipher yang berbeda mungkin memerlukan panjang kunci yang berbeda untuk mencapai tingkat kekuatan enkripsi yang sama. Cipher RSA yang digunakan untuk enkripsi kunci publik, misalnya, hanya dapat menggunakan subset dari semua nilai yang mungkin untuk kunci dengan panjang tertentu, karena sifat masalah matematika yang menjadi dasarnya. Cipher lainnya, seperti yang digunakan untuk enkripsi kunci simetris, dapat menggunakan semua nilai yang mungkin untuk kunci dengan panjang tertentu, daripada subset dari nilai tersebut. Jadi kunci 128-bit untuk digunakan dengan cipher enkripsi kunci simetris akan memberikan enkripsi yang lebih kuat daripada kunci 128-bit untuk digunakan dengan cipher enkripsi kunci publik RSA. Perbedaan ini menjelaskan mengapa cipher enkripsi kunci publik RSA harus menggunakan kunci 512-bit (atau lebih lama) untuk dianggap kuat secara kriptografis, sedangkan cipher kunci simetris dapat mencapai tingkat kekuatan yang kira-kira sama dengan kunci 64-bit. Bahkan tingkat kekuatan ini mungkin rentan terhadap serangan dalam waktu dekat.

Karena kemampuan untuk secara diam-diam mencegat dan mendekripsi informasi terenkripsi secara historis merupakan aset militer yang signifikan, Pemerintah AS membatasi

ekspor perangkat lunak kriptografi, termasuk sebagian besar perangkat lunak yang mengizinkan penggunaan kunci enkripsi simetris yang lebih panjang dari 40 bit.

9.6 SERTIFIKAT DAN OTENTIKASI

Sertifikat adalah dokumen elektronik yang digunakan untuk mengidentifikasi individu, server, perusahaan, atau entitas lain dan untuk mengaitkan identitas itu dengan kunci publik. Seperti SIM, paspor, atau tanda pengenal pribadi lainnya yang umum digunakan, sertifikat memberikan bukti identitas seseorang yang diakui secara umum. Kriptografi kunci publik menggunakan sertifikat untuk mengatasi masalah peniruan identitas. Untuk mendapatkan SIM, Anda biasanya mengajukan permohonan ke lembaga pemerintah, seperti Departemen Kendaraan Bermotor, yang memverifikasi identitas Anda, kemampuan Anda mengemudi, alamat Anda, dan informasi lain sebelum menerbitkan SIM. Untuk mendapatkan ID pelajar, Anda mendaftar ke sekolah atau perguruan tinggi, yang melakukan pemeriksaan berbeda (seperti apakah Anda telah membayar uang sekolah) sebelum mengeluarkan ID. Untuk mendapatkan kartu perpustakaan, Anda mungkin hanya perlu memberikan nama dan tagihan listrik dengan alamat Anda.

Sertifikat bekerja dengan cara yang sama seperti bentuk identifikasi yang sudah dikenal ini. Otoritas sertifikat (CA) adalah entitas yang memvalidasi identitas dan menerbitkan sertifikat. Mereka dapat berupa pihak ketiga yang independen atau organisasi yang menjalankan perangkat lunak server penerbit sertifikat mereka sendiri (seperti Sistem Sertifikat Red Hat). Metode yang digunakan untuk memvalidasi identitas berbeda-beda tergantung pada kebijakan CA yang diberikan-sama seperti metode untuk memvalidasi bentuk identifikasi lainnya bervariasi tergantung pada siapa yang mengeluarkan ID dan tujuan penggunaannya. Secara umum, sebelum menerbitkan sertifikat, CA harus menggunakan prosedur verifikasi yang dipublikasikan untuk jenis sertifikat tersebut guna memastikan bahwa entitas yang meminta sertifikat sebenarnya adalah yang diklaimnya. Sertifikat yang dikeluarkan oleh CA mengikat kunci publik tertentu ke nama entitas yang diidentifikasi oleh sertifikat (seperti nama karyawan atau server). Sertifikat membantu mencegah penggunaan kunci publik palsu untuk peniruan identitas. Hanya kunci publik yang disertifikasi oleh sertifikat yang akan bekerja dengan kunci privat terkait yang dimiliki oleh entitas yang diidentifikasi oleh sertifikat.

Selain kunci publik, sertifikat selalu menyertakan nama entitas yang diidentifikasi, tanggal kedaluwarsa, nama CA yang mengeluarkan sertifikat, nomor seri, dan informasi lainnya. Yang terpenting, sertifikat selalu menyertakan tanda tangan digital dari CA yang menerbitkan. Tanda tangan digital CA memungkinkan sertifikat berfungsi sebagai "surat pengantar" bagi pengguna yang mengetahui dan mempercayai CA tetapi tidak mengetahui entitas yang diidentifikasi oleh sertifikat.

Otentikasi Mengonfirmasi Identitas:

Otentikasi adalah proses konfirmasi identitas. Dalam konteks interaksi jaringan, otentikasi melibatkan identifikasi percaya diri dari satu pihak oleh pihak lain. Otentikasi melalui jaringan dapat mengambil banyak bentuk. Sertifikat adalah salah satu cara untuk mendukung otentikasi.

Interaksi jaringan biasanya terjadi antara klien, seperti perangkat lunak browser yang berjalan pada komputer pribadi, dan server, seperti perangkat lunak dan perangkat keras yang digunakan untuk meng-host situs Web. Otentikasi klien mengacu pada identifikasi klien secara meyakinkan oleh server (yaitu, identifikasi orang yang dianggap menggunakan perangkat lunak klien). Otentikasi server mengacu pada identifikasi server oleh klien (yaitu, identifikasi organisasi yang dianggap bertanggung jawab atas server di alamat jaringan tertentu).

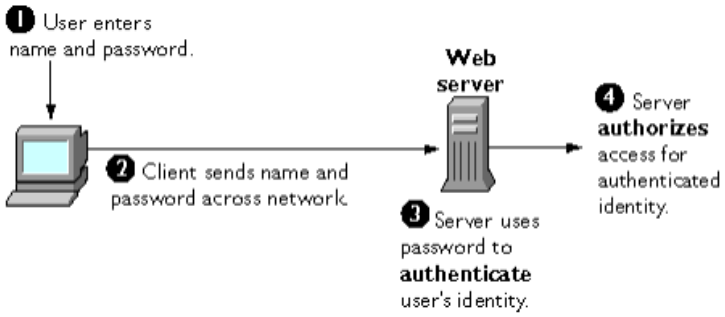
Otentikasi klien dan server bukan satu-satunya bentuk otentikasi yang didukung oleh sertifikat. Misalnya, tanda tangan digital pada pesan email, dikombinasikan dengan sertifikat yang mengidentifikasi pengirim, memberikan bukti kuat bahwa orang yang diidentifikasi oleh sertifikat itu memang mengirim pesan itu. Demikian pula, tanda tangan digital pada formulir HTML, dikombinasikan dengan sertifikat yang mengidentifikasi penandatangan, dapat memberikan bukti, setelah fakta, bahwa orang yang diidentifikasi oleh sertifikat itu setuju dengan isi formulir. Selain otentikasi, tanda tangan digital dalam kedua kasus memastikan tingkat non-penolakan-yaitu, tanda tangan digital mempersulit penandatangan untuk mengklaim kemudian tidak mengirim email atau formulir. Otentikasi klien adalah elemen penting dari keamanan jaringan di sebagian besar intranet atau ekstranet. Bagian yang mengikuti kontras dua bentuk otentikasi klien:

- Otentikasi Berbasis Sandi. Hampir semua perangkat lunak server mengizinkan otentikasi klien melalui nama dan kata sandi. Misalnya, server mungkin mengharuskan pengguna untuk mengetikkan nama dan kata sandi sebelum memberikan akses ke server. Server menyimpan daftar nama dan kata sandi; jika nama tertentu ada dalam daftar, dan jika pengguna mengetikkan kata sandi yang benar, server memberikan akses.
- Otentikasi Berbasis Sertifikat. Otentikasi klien berdasarkan sertifikat adalah bagian dari protokol SSL. Klien secara digital menandatangani sepotong data yang dihasilkan secara acak dan mengirimkan sertifikat dan data yang ditandatangani melalui jaringan. Server menggunakan teknik kriptografi kunci publik untuk memvalidasi tanda tangan dan mengonfirmasi validitas sertifikat.

Otentikasi Berbasis Kata Sandi

Gambar 9.2 menunjukkan langkah-langkah dasar yang terlibat dalam otentikasi klien dengan menggunakan nama dan kata sandi. Gambar 9.2 mengasumsikan sebagai berikut:

- Pengguna telah memutuskan untuk mempercayai server, baik tanpa otentikasi atau berdasarkan otentikasi server melalui SSL.
- Pengguna telah meminta sumber daya yang dikendalikan oleh server.
- Server memerlukan otentikasi klien sebelum mengizinkan akses ke sumber daya yang diminta.



Gambar 9.2 Langkah-langkah yang terlibat dalam otentikasi klien

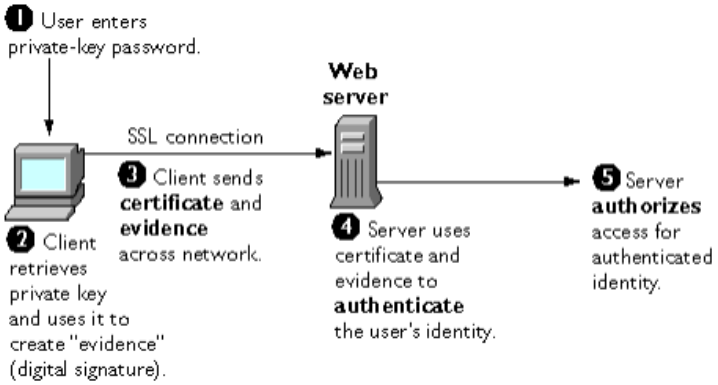
Ini adalah langkah-langkah yang ditunjukkan pada Gambar 9.2:

1. Menanggapi permintaan otentikasi dari server, klien menampilkan kotak dialog yang meminta nama pengguna dan kata sandi untuk server itu. Pengguna harus memberikan nama dan kata sandi secara terpisah untuk setiap server baru yang ingin digunakan pengguna selama sesi kerja.
2. Klien mengirimkan nama dan kata sandi melalui jaringan, baik secara jelas atau melalui koneksi SSL terenkripsi.
3. Server mencari nama dan kata sandi di basis data kata sandi lokalnya dan, jika cocok, menerimanya sebagai bukti yang mengotentikasi identitas pengguna.
4. Server menentukan apakah pengguna yang diidentifikasi diizinkan untuk mengakses sumber daya yang diminta, dan jika demikian, memungkinkan klien untuk mengaksesnya.

Dengan pengaturan ini, pengguna harus memberikan kata sandi baru untuk setiap server, dan administrator harus melacak nama dan kata sandi untuk setiap pengguna, biasanya di server terpisah. Implementasi yang tepat tidak menyimpan kata sandi dalam teks biasa. Alih-alih itu menggabungkan kata sandi dengan nilai per pengguna acak (disebut "garam") dan menyimpan nilai hash dari hasilnya bersama dengan garamnya. Ini membuat beberapa jenis serangan brute force lebih sulit. Seperti yang ditunjukkan pada bagian berikutnya, salah satu keuntungan dari otentikasi berbasis sertifikat adalah dapat digunakan untuk menggantikan tiga langkah pertama pada Gambar 9.2 dengan mekanisme yang memungkinkan pengguna untuk memberikan hanya satu kata sandi (yang tidak dikirim ke seluruh jaringan) dan memungkinkan administrator untuk mengontrol otentikasi pengguna secara terpusat.

Otentikasi Berbasis Sertifikat

Gambar 9.3 menunjukkan cara kerja otentikasi klien menggunakan sertifikat dan protokol SSL. Untuk mengautentikasi pengguna ke server, klien secara digital menandatangani sepotong data yang dihasilkan secara acak dan mengirimkan sertifikat dan data yang ditandatangani melalui jaringan. Untuk tujuan diskusi ini, tanda tangan digital yang terkait dengan beberapa data dapat dianggap sebagai bukti yang diberikan oleh klien ke server. Server mengotentikasi identitas pengguna pada kekuatan bukti ini. Seperti Gambar 9.2, Gambar 9.3 mengasumsikan bahwa pengguna telah memutuskan untuk mempercayai server dan telah meminta sumber daya, dan bahwa server telah meminta otentikasi klien dalam proses mengevaluasi apakah akan memberikan akses ke sumber daya yang diminta.



Gambar 9.3 Proses jika klien memiliki sertifikat valid untuk identifikasi klien ke server

Berbeda dengan proses yang ditunjukkan pada Gambar 9.2, proses yang ditunjukkan pada Gambar 9.3 membutuhkan penggunaan SSL. Gambar 9.3 juga mengasumsikan bahwa klien memiliki sertifikat yang valid yang dapat digunakan untuk mengidentifikasi klien ke server. Otentikasi berbasis sertifikat umumnya dianggap lebih disukai daripada otentikasi berbasis kata sandi karena didasarkan pada gandum yang dimiliki pengguna (kunci pribadi) serta apa yang diketahui pengguna (kata sandi yang melindungi kunci pribadi). Namun, penting untuk dicatat bahwa kedua asumsi ini benar hanya jika personel yang tidak berwenang belum memperoleh akses ke mesin atau kata sandi pengguna, kata sandi untuk basis data kunci pribadi perangkat lunak klien telah ditetapkan, dan perangkat lunak diatur untuk meminta kata sandi pada interval frekuensi yang wajar.

Baik otentikasi berbasis kata sandi maupun otentikasi berbasis sertifikat tidak mengatasi masalah keamanan yang terkait dengan akses fisik ke mesin atau kata sandi individual. Kriptografi kunci publik hanya dapat memverifikasi bahwa kunci pribadi yang digunakan untuk menandatangani beberapa data sesuai dengan kunci publik dalam sertifikat. Merupakan tanggung jawab pengguna untuk melindungi keamanan fisik mesin dan menjaga kerahasiaan kata sandi kunci pribadi. Ini adalah langkah-langkah yang ditunjukkan pada Gambar 9.3:

1. Perangkat lunak klien, seperti Communicator, memelihara basis data kunci privat yang sesuai dengan kunci publik yang diterbitkan dalam sertifikat apa pun yang diterbitkan untuk klien tersebut. Klien meminta kata sandi ke database ini saat pertama kali klien perlu mengaksesnya selama sesi tertentu-misalnya, pertama kali pengguna mencoba mengakses server berkemampuan SSL yang memerlukan otentikasi klien berbasis sertifikat. Setelah memasukkan kata sandi ini sekali, pengguna tidak perlu memasukkannya lagi selama sisa sesi, bahkan saat mengakses server lain yang mendukung SSL.
2. Klien membuka kunci basis data kunci privat, mengambil kunci privat untuk sertifikat pengguna, dan menggunakan kunci privat tersebut untuk menandatangani secara digital beberapa data yang telah dibuat secara acak untuk tujuan ini berdasarkan input dari klien dan server . Data ini dan tanda tangan digital merupakan "bukti" validitas kunci pribadi. Tanda tangan digital hanya dapat dibuat dengan kunci pribadi itu dan

dapat divalidasi dengan kunci publik yang sesuai terhadap data yang ditandatangani, yang unik untuk sesi SSL.

3. Klien mengirimkan sertifikat pengguna dan bukti (sepotong data yang dihasilkan secara acak yang telah ditandatangani secara digital) melalui jaringan.
4. Server menggunakan sertifikat dan bukti untuk mengotentikasi identitas pengguna.

Pada titik ini, server secara opsional dapat melakukan tugas autentikasi lainnya, seperti memeriksa apakah sertifikat yang diberikan oleh klien disimpan dalam entri pengguna di direktori LDAP. Server kemudian melanjutkan untuk mengevaluasi apakah pengguna yang diidentifikasi diizinkan untuk mengakses sumber daya yang diminta. Proses evaluasi ini dapat menggunakan berbagai mekanisme otorisasi standar, berpotensi menggunakan informasi tambahan dalam direktori LDAP, database perusahaan, dan sebagainya. Jika hasil evaluasi positif, server mengizinkan klien untuk mengakses sumber daya yang diminta.

Seperti yang Anda lihat dengan membandingkan Gambar 9.3 dengan Gambar 9.2, sertifikat menggantikan bagian otentikasi dari interaksi antara klien dan server. Alih-alih mengharuskan pengguna untuk mengirim kata sandi di seluruh jaringan sepanjang hari, sistem masuk tunggal mengharuskan pengguna untuk memasukkan kata sandi basis data kunci pribadi sekali saja, tanpa mengirimkannya ke seluruh jaringan. Selama sisa sesi, klien menyajikan sertifikat pengguna untuk mengautentikasi pengguna ke setiap server baru yang ditemuinya. Mekanisme otorisasi yang ada berdasarkan identitas pengguna yang diautentikasi tidak terpengaruh.

9.7 BAGAIMANA SERTIFIKAT DIGUNAKAN?

- Jenis Sertifikat
- Protokol SSL
- Email yang Ditandatangani dan Dienkripsi
- Penandatanganan Formulir
- Sistem Masuk Tunggal
- Jenis Sertifikat Penandatanganan Obyek

Lima jenis sertifikat yang umum digunakan dengan produk Red Hat:

- Sertifikat SSL klien: Digunakan untuk mengidentifikasi klien ke server melalui SSL (otentikasi klien). Biasanya, identitas klien diasumsikan sama dengan identitas manusia, seperti karyawan di suatu perusahaan. Lihat "Otentikasi Berbasis Sertifikat", untuk penjelasan tentang cara sertifikat SSL klien digunakan untuk otentikasi klien. Sertifikat SSL klien juga dapat digunakan untuk penandatanganan formulir dan sebagai bagian dari solusi sistem masuk tunggal.
- Contoh: Bank memberi pelanggan sertifikat SSL klien yang memungkinkan server bank mengidentifikasi pelanggan tersebut dan mengizinkan akses ke akun pelanggan. Perusahaan mungkin memberi karyawan baru sertifikat SSL klien yang memungkinkan server perusahaan mengidentifikasi karyawan tersebut dan mengotorisasi akses ke server perusahaan.
- Sertifikat SSL server: Digunakan untuk mengidentifikasi server ke klien melalui SSL (otentikasi server). Otentikasi server dapat digunakan dengan atau tanpa otentikasi klien. Otentikasi server adalah persyaratan untuk sesi SSL terenkripsi.

Contoh: Situs internet yang terlibat dalam perdagangan elektronik (umumnya dikenal sebagai e-niaga) biasanya mendukung otentikasi server berbasis sertifikat, minimal, untuk membuat sesi SSL terenkripsi dan untuk meyakinkan pelanggan bahwa mereka berurusan dengan situs web yang diidentifikasi dengan perusahaan tertentu. Sesi SSL terenkripsi memastikan bahwa informasi pribadi yang dikirim melalui jaringan, seperti nomor kartu kredit, tidak dapat dengan mudah disadap.

- Sertifikat S/MIME: Digunakan untuk email yang ditandatangani dan dienkripsi. Seperti halnya sertifikat SSL klien, identitas klien biasanya diasumsikan sama dengan identitas manusia, seperti karyawan di suatu perusahaan. Satu sertifikat dapat digunakan sebagai sertifikat S/MIME dan sertifikat SSL. Sertifikat S/MIME juga dapat digunakan untuk penandatanganan formulir dan sebagai bagian dari solusi sistem masuk tunggal.
- Contoh: Perusahaan menyebarkan gabungan S/MIME dan sertifikat SSL semata-mata untuk tujuan mengautentikasi identitas karyawan, sehingga mengizinkan email yang ditandatangani dan otentikasi SSL klien tetapi bukan email terenkripsi. Perusahaan lain menerbitkan sertifikat S/MIME semata-mata untuk tujuan menandatangani dan mengenkripsi email yang berhubungan dengan masalah keuangan atau hukum yang sensitif.
- Sertifikat penandatanganan objek: Digunakan untuk mengidentifikasi penanda kode Java, skrip JavaScript, atau file bertanda tangan lainnya. Untuk informasi lebih lanjut, lihat "Penandatanganan Objek".
- Contoh: Perusahaan perangkat lunak menandatangani perangkat lunak yang didistribusikan melalui Internet untuk memberikan jaminan kepada pengguna bahwa perangkat lunak tersebut adalah produk yang sah dari perusahaan tersebut. Menggunakan sertifikat dan tanda tangan digital dengan cara ini juga memungkinkan pengguna untuk mengidentifikasi dan mengontrol jenis akses yang dimiliki perangkat lunak yang diunduh ke komputer mereka.
- sertifikat CA. Digunakan untuk mengidentifikasi CA. Perangkat lunak klien dan server menggunakan sertifikat CA untuk menentukan sertifikat lain yang dapat dipercaya. Untuk informasi lebih lanjut .
- Contoh: Sertifikat CA yang disimpan di Communicator menentukan sertifikat lain yang dapat diautentikasi oleh salinan Communicator. Administrator dapat menerapkan beberapa aspek kebijakan keamanan perusahaan dengan mengontrol sertifikat CA yang disimpan dalam salinan Communicator setiap pengguna.
- Protokol SSL

Protokol Secure Sockets Layer (SSL) adalah seperangkat aturan yang mengatur otentikasi server, otentikasi klien, dan komunikasi terenkripsi antara server dan klien. SSL banyak digunakan di Internet, terutama untuk interaksi yang melibatkan pertukaran informasi rahasia seperti nomor kartu kredit. SSL membutuhkan sertifikat SSL server, minimal. Sebagai bagian dari proses "jabat tangan" awal, server menyajikan sertifikatnya kepada klien untuk mengotentikasi identitas server. Proses otentikasi menggunakan enkripsi kunci publik dan tanda tangan digital untuk mengonfirmasi bahwa server sebenarnya adalah server yang diklaimnya. Setelah server diautentikasi, klien dan server menggunakan teknik enkripsi kunci simetris, yang sangat cepat, untuk mengenkripsi semua informasi yang mereka tukarkan

untuk sisa sesi dan untuk mendeteksi gangguan yang mungkin terjadi. Server secara opsional dapat dikonfigurasi untuk memerlukan otentikasi klien serta otentikasi server. Dalam hal ini, setelah otentikasi server berhasil diselesaikan, klien juga harus menunjukkan sertifikatnya ke server untuk mengotentikasi identitas klien sebelum sesi SSL terenkripsi dapat dibuat. Untuk gambaran umum tentang otentikasi klien melalui SSL dan perbedaannya dari otentikasi berbasis kata sandi.

Email yang Ditandatangani dan Dienkripsi:

Beberapa program email (termasuk Messenger, yang merupakan bagian dari Communicator) mendukung email yang ditandatangani secara digital dan dienkripsi menggunakan protokol yang diterima secara luas yang dikenal sebagai Secure Multipurpose Internet Mail Extension (S/MIME). Menggunakan S/MIME untuk menandatangani atau mengenkripsi pesan email mengharuskan pengirim pesan memiliki sertifikat S/MIME. Pesan email yang menyertakan tanda tangan digital memberikan beberapa jaminan bahwa pesan itu sebenarnya dikirim oleh orang yang namanya muncul di header pesan, sehingga memberikan otentikasi pengirim. Jika tanda tangan digital tidak dapat divalidasi oleh perangkat lunak email di pihak penerima, pengguna akan diberi tahu. Tanda tangan digital unik untuk pesan yang menyertainya. Jika pesan yang diterima berbeda dari pesan yang dikirim-bahkan dengan penambahan atau penghapusan koma-tanda tangan digital tidak dapat divalidasi. Oleh karena itu, email yang ditandatangani juga memberikan jaminan bahwa email tersebut tidak dirusak. Sebagaimana dibahas di awal dokumen ini, jaminan semacam ini dikenal sebagai nonrepudiation. Dengan kata lain, email yang ditandatangani mempersulit pengirim untuk menyangkal telah mengirim pesan. Ini penting untuk banyak bentuk komunikasi bisnis. S/MIME juga memungkinkan untuk mengenkripsi pesan email. Ini juga penting bagi beberapa pengguna bisnis. Namun, menggunakan enkripsi untuk email memerlukan perencanaan yang matang. Jika penerima pesan email terenkripsi kehilangan kunci pribadinya dan tidak memiliki akses ke salinan cadangan kunci, misalnya, pesan terenkripsi tidak akan pernah dapat didekripsi.

Penandatanganan Formulir:

Banyak jenis e-commerce membutuhkan kemampuan untuk memberikan bukti yang terus-menerus bahwa seseorang telah mengesahkan transaksi. Meskipun SSL menyediakan otentikasi klien sementara selama koneksi SSL, SSL tidak menyediakan otentikasi terus-menerus untuk transaksi yang mungkin terjadi selama koneksi tersebut. S/MIME menyediakan otentikasi terus-menerus untuk email, tetapi e-commerce sering kali melibatkan pengisian formulir di halaman web daripada mengirim email. Teknologi Red Hat yang dikenal sebagai penandatanganan formulir menjawab kebutuhan akan autentikasi transaksi keuangan yang terus-menerus. Penandatanganan formulir memungkinkan pengguna untuk mengaitkan tanda tangan digital dengan data berbasis web yang dihasilkan sebagai hasil transaksi, seperti pesanan pembelian atau dokumen keuangan lainnya. Kunci pribadi yang terkait dengan sertifikat SSL klien atau sertifikat S/MIME dapat digunakan untuk tujuan ini. Saat pengguna mengklik tombol Kirim pada formulir berbasis web yang mendukung penandatanganan formulir, kotak dialog akan muncul yang menampilkan teks yang tepat untuk ditandatangani. Perancang formulir dapat menentukan sertifikat yang harus digunakan atau mengizinkan pengguna untuk memilih sertifikat dari antara sertifikat SSL dan S/MIME klien yang diinstal di

Communicator. Ketika pengguna mengklik OK, teks ditandatangani, dan teks dan tanda tangan digital dikirimkan ke server. Server kemudian dapat menggunakan utilitas Red Hat yang disebut Alat Verifikasi Tanda Tangan untuk memvalidasi tanda tangan digital.

Sistem Masuk Tunggal:

Pengguna jaringan sering diminta untuk mengingat beberapa kata sandi untuk berbagai layanan yang mereka gunakan. Misalnya, pengguna mungkin harus mengetikkan kata sandi yang berbeda untuk masuk ke jaringan, mengumpulkan email, menggunakan layanan direktori, menggunakan program kalender perusahaan, dan mengakses berbagai server. Beberapa kata sandi adalah sakit kepala yang berkelanjutan bagi pengguna dan administrator sistem. Pengguna mengalami kesulitan melacak kata sandi yang berbeda, cenderung memilih kata sandi yang buruk, dan cenderung menuliskannya di tempat yang jelas. Administrator harus melacak database kata sandi terpisah di setiap server dan menangani potensi masalah keamanan yang terkait dengan fakta bahwa kata sandi dikirim melalui jaringan secara rutin dan sering.

Memecahkan masalah ini memerlukan beberapa cara bagi pengguna untuk masuk sekali, menggunakan satu kata sandi, dan mendapatkan akses terautentikasi ke semua sumber daya jaringan yang diizinkan pengguna untuk digunakan-tanpa mengirim kata sandi apa pun melalui jaringan. Kemampuan ini dikenal sebagai sistem masuk tunggal. Baik sertifikat SSL klien maupun sertifikat S/MIME dapat memainkan peran penting dalam solusi sistem masuk tunggal yang komprehensif. Misalnya, satu bentuk sistem masuk tunggal yang didukung oleh produk Red Hat bergantung pada otentikasi klien SSL. Seorang pengguna dapat masuk sekali, menggunakan satu kata sandi ke basis data kunci pribadi klien lokal, dan mendapatkan akses terotentikasi ke semua server berkemampuan SSL yang diizinkan untuk digunakan oleh pengguna-tanpa mengirim kata sandi apa pun melalui jaringan. Pendekatan ini menyederhanakan akses bagi pengguna, karena mereka tidak perlu memasukkan kata sandi untuk setiap server baru. Ini juga menyederhanakan manajemen jaringan, karena administrator dapat mengontrol akses dengan mengontrol daftar otoritas sertifikat (CA) daripada daftar pengguna dan kata sandi yang lebih panjang. Selain menggunakan sertifikat, solusi masuk tunggal yang lengkap harus memenuhi kebutuhan untuk beroperasi dengan sistem perusahaan, seperti sistem operasi yang mendasarinya, yang mengandalkan kata sandi atau bentuk autentikasi lainnya.

Penandatanganan Objek

Komunikator mendukung seperangkat alat dan teknologi yang disebut penandatanganan objek. Penandatanganan objek menggunakan teknik standar kriptografi kunci publik untuk memungkinkan pengguna mendapatkan informasi yang dapat dipercaya tentang kode yang mereka unduh dengan cara yang sama seperti mereka dapat memperoleh informasi yang dapat diandalkan tentang perangkat lunak yang dibungkus dengan shrink. Yang paling penting, penandatanganan objek membantu pengguna dan administrator jaringan menerapkan keputusan tentang perangkat lunak yang didistribusikan melalui intranet atau Internet-misalnya, apakah mengizinkan applet Java yang ditandatangani oleh entitas tertentu untuk menggunakan kemampuan komputer tertentu pada mesin pengguna tertentu. "Objek" yang ditandatangani dengan teknologi penandatanganan objek dapat berupa applet atau kode Java lainnya, skrip JavaScript, plug-in, atau jenis file apa pun. "Tanda tangan" adalah

tanda tangan digital. Objek yang ditandatangani dan tanda tangannya biasanya disimpan dalam file khusus yang disebut file JAR. Pengembang perangkat lunak dan orang lain yang ingin menandatangani file menggunakan teknologi penandatanganan objek harus terlebih dahulu mendapatkan sertifikat penandatanganan objek.

9.8 INFRASTRUKTUR KUNCI PUBLIK (PKI)

Infrastruktur kunci publik (PKI) mendukung distribusi dan identifikasi kunci enkripsi publik, memungkinkan pengguna dan komputer untuk bertukar data dengan aman melalui jaringan seperti Internet dan memverifikasi identitas pihak lain. Infrastruktur kunci publik (PKI) mendukung distribusi dan identifikasi kunci enkripsi publik, memungkinkan pengguna dan komputer untuk bertukar data dengan aman melalui jaringan seperti Internet dan memverifikasi identitas pihak lain.

Tanpa PKI, informasi sensitif masih dapat dienkripsi (memastikan kerahasiaan) dan dipertukarkan, tetapi tidak akan ada jaminan identitas (otentikasi) pihak lain. Segala bentuk data sensitif yang dipertukarkan melalui Internet bergantung pada PKI untuk keamanan.

PKI khas terdiri dari perangkat keras, perangkat lunak, kebijakan dan standar untuk mengelola pembuatan, administrasi, distribusi dan pencabutan kunci dan sertifikat digital. Sertifikat digital adalah inti dari PKI karena mereka menegaskan identitas subjek sertifikat dan mengikat identitas itu ke kunci publik yang terkandung dalam sertifikat. PKI tipikal mencakup elemen-elemen kunci berikut:

- Pihak tepercaya, yang disebut otoritas sertifikat (CA), bertindak sebagai akar kepercayaan dan menyediakan layanan yang mengotentikasi identitas individu, komputer, dan entitas lain
- Otoritas pendaftaran, sering disebut CA bawahan, disertifikasi oleh CA root untuk menerbitkan sertifikat untuk penggunaan khusus yang diizinkan oleh root
- Basis data sertifikat, yang menyimpan permintaan dan penerbitan sertifikat serta mencabut sertifikat
- Sebuah toko sertifikat, yang berada di komputer lokal sebagai tempat untuk menyimpan sertifikat dan kunci pribadi yang dikeluarkan

CA mengeluarkan sertifikat digital kepada entitas dan individu setelah memverifikasi identitas mereka. Itu menandatangani sertifikat ini menggunakan kunci pribadinya; kunci publiknya tersedia untuk semua pihak yang berkepentingan dalam sertifikat CA yang ditandatangani sendiri. CA menggunakan sertifikat root tepercaya ini untuk membuat "rantai kepercayaan" -- banyak sertifikat root disematkan di browser Web sehingga mereka memiliki kepercayaan bawaan dari CA tersebut. Server web, klien email, ponsel pintar, dan banyak jenis perangkat keras dan perangkat lunak lainnya juga mendukung PKI dan berisi sertifikat root tepercaya dari CA utama. Bersama dengan kunci publik entitas atau individu, sertifikat digital berisi informasi tentang algoritme yang digunakan untuk membuat tanda tangan, orang atau entitas yang diidentifikasi, tanda tangan digital CA yang memverifikasi data subjek dan menerbitkan sertifikat, tujuan kunci publik enkripsi, tanda tangan dan penandatanganan sertifikat, serta rentang tanggal di mana sertifikat dapat dianggap valid.

PKI menyediakan rantai kepercayaan, sehingga identitas pada jaringan dapat diverifikasi. Namun, seperti rantai lainnya, PKI hanya sekuat mata rantai terlemahnya. Ada

berbagai standar yang mencakup aspek-aspek PKI -- seperti Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC2527) -- tetapi tidak ada badan pengatur utama yang menerapkan standar ini. Meskipun CA sering disebut sebagai "pihak ketiga yang tepercaya", kekurangan dalam prosedur keamanan berbagai CA dalam beberapa tahun terakhir telah membahayakan kepercayaan di seluruh PKI tempat Internet bergantung. Jika satu CA dikompromikan, keamanan seluruh PKI terancam. Misalnya, pada tahun 2011, vendor browser web terpaksa memasukkan semua sertifikat yang dikeluarkan oleh CA DigiNotar Belanda ke daftar hitam setelah lebih dari 500 sertifikat palsu ditemukan.

9.9 OTORITAS PENDAFTARAN

Otoritas pendaftaran (RA) adalah otoritas dalam jaringan yang memverifikasi permintaan pengguna untuk sertifikat digital dan memberi tahu otoritas sertifikat (CA) untuk menerbitkannya. Otoritas pendaftaran (RA) adalah otoritas dalam jaringan yang memverifikasi permintaan pengguna untuk sertifikat digital dan memberi tahu otoritas sertifikat (CA) untuk menerbitkannya. RA adalah bagian dari infrastruktur kunci publik (PKI), sistem jaringan yang memungkinkan perusahaan dan pengguna untuk bertukar informasi dan uang dengan aman dan terjamin. Sertifikat digital berisi kunci publik yang digunakan untuk mengenkripsi dan mendekripsi pesan dan tanda tangan digital.

Sertifikat tepercaya biasanya digunakan untuk membuat koneksi aman ke server melalui Internet. Sertifikat diperlukan untuk menghindari kasus bahwa pihak jahat yang kebetulan berada di jalur ke server target berpura-pura menjadi target. Skenario seperti itu biasanya disebut sebagai serangan man-in-the-middle. Klien menggunakan sertifikat CA untuk memverifikasi tanda tangan CA pada sertifikat server, sebagai bagian dari pemeriksaan sebelum membuat sambungan aman. Biasanya, perangkat lunak klien—misalnya, browser—menyertakan serangkaian sertifikat CA tepercaya. Itu masuk akal sebanyak pengguna perlu memercayai perangkat lunak klien mereka: Klien yang jahat atau disusupi dapat melewati pemeriksaan keamanan apa pun dan masih membodohi penggunanya agar percaya sebaliknya.

Pelanggan CA adalah administrator server yang memerlukan sertifikat yang akan diberikan server mereka kepada klien. CA komersial mengenakan biaya untuk menerbitkan sertifikat, dan pelanggan mereka mengharapkan sertifikat CA disertakan oleh sebagian besar browser web, sehingga koneksi aman ke server bersertifikat bekerja dengan lancar di luar kotak. Jumlah browser web dan perangkat serta aplikasi lain yang mempercayai otoritas sertifikat tertentu disebut sebagai ubiquity. Mozilla, yang merupakan organisasi nirlaba, mendistribusikan beberapa sertifikat CA komersial dengan produknya.[1] Sementara Mozilla mengembangkan kebijakan mereka sendiri, CA/Forum Browser mengembangkan pedoman serupa untuk kepercayaan CA. Sertifikat CA tunggal dapat dibagikan di antara beberapa CA atau pengecernya. Sertifikat CA root mungkin menjadi dasar untuk mengeluarkan beberapa sertifikat CA perantara dengan persyaratan validasi yang bervariasi.

Selain CA komersial, beberapa penyedia menerbitkan sertifikat digital kepada publik tanpa biaya; contoh yang patut diperhatikan adalah CAcert. Institusi besar atau entitas pemerintah mungkin memiliki PKI sendiri, masing-masing termasuk CA mereka sendiri. Secara

formal, situs apa pun yang menggunakan sertifikat yang ditandatangani sendiri juga bertindak sebagai CA-nya sendiri. Bagaimanapun, klien yang layak memungkinkan pengguna untuk menambah atau menghapus sertifikat CA sesuka hati. Meskipun sertifikat server biasanya bertahan untuk waktu yang agak singkat, sertifikat CA bertahan lebih lama, [2] jadi, untuk server yang sering dikunjungi, lebih sedikit kesalahan untuk mengimpor dan memercayai CA yang menerbitkan sertifikatnya daripada mengonfirmasi pengecualian keamanan setiap waktu sertifikat server diperbarui.

Penggunaan sertifikat tepercaya yang lebih jarang adalah untuk mengenkripsi atau menandatangani pesan. CA juga mengeluarkan sertifikat pengguna akhir, yang dapat digunakan dengan S/MIME. Namun, enkripsi memerlukan kunci publik penerima dan, karena penulis dan penerima pesan terenkripsi mungkin saling mengenal, kegunaan pihak ketiga yang tepercaya tetap terbatas pada verifikasi tanda tangan dari pesan yang dikirim ke milis publik.

9.10 APA YANG HARUS DILAKUKAN

Sistem pertahanan terhadap serangan Internet telah berkembang berdampingan dengan agresi dalam semacam versi serius dari serial kartun "Spy vs. Spy" yang dibuat terkenal oleh Mad Magazine. Tiga tindakan penting yang tersedia untuk individu dan bisnis, betapapun kecilnya, adalah 1) penggunaan sistem komputer secara disiplin termasuk kata sandi dan kontrol email yang cermat, 2) pemasangan dan peningkatan firewall antara jaringan internal dan Internet, 3) kewaspadaan terhadap berita. tentang virus dan pelanggaran baru dan segera melaksanakan rekomendasi publik, dan 4) pelaporan pelanggaran segera kepada pihak berwenang segera setelah terdeteksi.

Pemilik bisnis memiliki tanggung jawab utama untuk menolak akses ke sistemnya kepada individu yang seharusnya tidak menggunakannya. Ini biasanya dicapai dengan menggunakan kontrol kata sandi. Di lingkungan modern kita diharuskan menggunakan terlalu banyak kata sandi. Tidak mengherankan, kami memilih salah satu yang kami sukai dan cenderung bertahan dengannya. Kami menggunakan kata sandi yang sama untuk sejumlah akun online yang berbeda, di rumah, di kantor. Penangkapan satu di suatu tempat dapat menyebabkan penggunaannya di tempat lain. Dalam kasus di mana disiplin yang baik ditegakkan, kata sandi baru dikeluarkan secara berkala—tetapi orang cenderung melupakannya, dengan konsekuensi bahwa kata sandi itu sering dicoret-coret di monitor komputer dengan pensil. Praktik ceroboh seperti itu, tentu saja, sebagian bertanggung jawab atas pelanggaran besar dan banyak kerusakan. Sebagian besar virus ditransmisikan sebagai lampiran email. Membuka lampiran dari pemancar email yang tidak dikenal umumnya merupakan ide yang buruk—bahkan ketika pesannya terdengar masuk akal. Aturan yang baik untuk diikuti dalam kasus seperti itu adalah jika pengirim benar-benar ingin saya membuka surat itu, dia akan menelepon. Keingintahuan yang menganggur menyebabkan banyak virus menyebar.

Sebagian besar usaha kecil dengan jaringan akan melibatkan perusahaan jasa untuk memelihara dan secara berkala memeriksa sistemnya atau akan ada staf internal yang mengelola fungsi tersebut. Firewall dan perangkat lunak pendeteksi virus memerlukan pemeliharaan dan peningkatan berkala. Kegagalan untuk melakukannya dapat membuka sistem perusahaan untuk spammer yang akan menggunakannya sebagai titik transmisi—

menggunakan kekuatan prosesor yang berharga dan akhirnya menyebabkan email perusahaan sendiri ditolak oleh orang lain—atau lebih buruk lagi. Paket pemantauan virus lama tidak akan menyadari worm baru, Trojan horse, dan bom logika. Ketika ada berita yang menunjukkan bahwa beberapa program perangkat lunak memiliki kelemahan besar, produsen perangkat lunak segera memiliki "tambalan" yang siap untuk memperbaiki kerentanan. Mengunduh dan memasang tambalan semacam itu akan merepotkan, tetapi kegagalan untuk melakukannya mungkin akan lebih mahal. Bayar saya sekarang atau bayar saya nanti! Beberapa situs Web menyediakan peringatan virus gratis dan patch antivirus yang dapat diunduh untuk browser Web. Contohnya termasuk www.symantec.com/avcenter dan www.ciac.org. Institut Keamanan Komputer menyediakan survei tahunan tentang pelanggaran keamanan di www.gocsi.com.

Sumber daya lain yang bermanfaat adalah National Computer Security Association (www.ncsa.com), yang memberikan tip tentang keamanan Internet untuk pemilik bisnis dan menyediakan definisi istilah teknologi tinggi.

Pelanggaran sistem harus segera dilaporkan. Bisnis dapat melakukannya dengan menghubungi US-CERT (Tim Kesiapan Darurat Komputer Amerika Serikat). Organisasi federal ini, yang dibentuk pada tahun 2003, bekerja dengan komunitas Internet untuk meningkatkan kesadaran akan masalah keamanan dan mengatur respons terhadap ancaman keamanan. Situs web CERT memposting peringatan keamanan terbaru dan juga menyediakan dokumen, alat, dan seminar pelatihan yang terkait dengan keamanan. Terakhir, CERT menawarkan bantuan teknis 24 jam jika terjadi pelanggaran keamanan Internet. Pemilik usaha kecil yang menghubungi CERT tentang masalah keamanan akan diminta untuk memberikan alamat Internet perusahaan mereka, model komputer yang terpengaruh, jenis sistem operasi dan perangkat lunak yang digunakan, dan langkah-langkah keamanan yang ada.

Untuk sebagian besar usaha kecil, Internet adalah sumber daya yang berharga. Upaya yang diperlukan untuk bermain sesuai aturan relatif rendah. Biaya, minimal dalam waktu, seringkali dalam dolar, bisa sangat tinggi bahkan untuk masalah kecil seperti server seseorang dibajak untuk spamming. Ketika virus menghancurkan disk yang menyimpan data berharga, biaya bisa meroket. Kehati-hatian, kewaspadaan, dan disiplin dapat mencegah masalah terburuk seperti itu. Oleh karena itu, kebijakan keamanan yang baik harus menjadi agenda utama pemilik bisnis.

9.11 RINGKASAN

Keamanan Internet adalah masalah yang menantang dan teknis untuk semua, Ini membutuhkan perhatian penuh dari para pakar TI dan konsensus di tingkat industri. Dalam unit ini konsep keamanan internet-siapa yang harus Anda percayai, etika penelitian internet, berbagai masalah internet lainnya, enkripsi dan dekripsi, sertifikat dan otentikasi, bagaimana sertifikat ini dapat digunakan dan apa yang harus dilakukan dibahas panjang lebar untuk memahami masalah ini dengan bantuan contoh dan ilustrasi yang relevan.

9.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)

- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Penulis)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew
- M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Publikasi Ruang)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

9.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Sifat internet yang terbuka membuat penting bagi bisnis untuk memperhatikan keamanan jaringan mereka.
b) Keamanan internet adalah tentang kepercayaan dari jauh.
c) Semua komunikasi melalui internet menggunakan Transmission on Control Protocol/Internet Protocol.
d) Sertifikat bekerja dengan cara yang sama seperti bentuk-bentuk identifikasi yang sudah dikenal ini.
e) Hampir semua perangkat lunak server mengizinkan otentikasi klien melalui nama dan kata sandi.

B. Isi Bagian yang Kosong:

i Internet..... adalah sub disiplin yang cocok di banyak disiplin ilmu.
ii Etika penelitian internet meliputi ..... dan standar profesional.

iii ..... adalah proses mengubah informasi sehingga tidak berwujud bagi siapa pun kecuali penerima independen.

iv Sertifikat adalah ..... digunakan untuk mengidentifikasi individu, server, perusahaan, atau entitas lain dan untuk mengaitkan identitas itu dengan kunci publik.

v SMIME artinya.....

9.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Etika Penelitian
2. Privasi dan kerahasiaan data, integritas data, masalah IP
3. Enkripsi
4. Dokumen elektronik
5. Ekstensi Surat Internet Serbaguna yang Aman

9.15 PERTANYAAN TERMINAL

1. Siapa yang harus Anda percayai dalam hal Keamanan Internet?
2. Apa yang dimaksud dengan etika penelitian internet?
3. Apa itu Enkripsi dan Dekripsi?
4. Tentukan sertifikat dan otentikasi.
5. Bagaimana sertifikat digunakan?

BAB 10
AKUNTABILITAS PENYEDIA LAYANAN

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan Akuntabilitas Penyedia Jasa
- Memahami peran Penyedia Layanan di Tingkat Internasional di berbagai negara
- Memahami masalah teknis dan hukum terkait Akuntabilitas Penyedia Layanan

10.1 PENGANTAR

Munculnya bentuk-bentuk baru komunikasi massa melalui teknologi telah menimbulkan hambatan dan tantangan regulasi. Mungkin salah satu isu yang paling sensitif dan bermasalah dari sudut pandang model ekonomi terkait dan konflik dengan hak konstitusional lainnya, terutama hak atas kebebasan berekspresi, berkaitan dengan mekanisme untuk menetapkan tanggung jawab. Seperti diketahui, penggunaan jaringan digital telah menggeser diskusi mengenai berbagai aspek tanggung jawab perdata ke pengaturan baru, dengan kesulitan yang menyertainya. Ketika datang ke lingkungan online, infrastruktur teknologi tampaknya tidak menimbulkan, setidaknya secara apriori, hambatan regulasi untuk pelaksanaan kebebasan berekspresi.

Awalnya, dengan proliferasi sistem papan buletin, dan kemudian dengan munculnya milis dan meluasnya penggunaan email, komunikasi pada dasarnya menjadi terdesentralisasi dan dikembangkan melalui protokol komunikasi yang memungkinkan pertukaran semacam itu. Tetapi dengan kemungkinan teknis yang memungkinkan pertukaran hal-hal tak berwujud melalui jaringan digital dan dalam beberapa tahun terakhir dengan booming yang disebut jaringan sosial, pentingnya regulasi infrastruktur ini untuk pelaksanaan hak menjadi semakin jelas. Entah bagaimana, fitur bersama dari tindakan komunikatif ini adalah kebutuhan akan infrastruktur teknologi. Infrastruktur ini, pada gilirannya, dioperasikan oleh penyedia layanan Internet, yang tidak hanya mengelola tetapi juga memiliki kekuatan untuk mengontrol aliran data di seluruh jaringan mereka.

Oleh karena itu, dari sudut pandang peraturan, penting untuk menetapkan kriteria tegas untuk memastikan bahwa netralitas bersih dipertahankan dan, dalam hal ini khususnya, pentingnya dan kebutuhan untuk menetapkan sistem yang akan memberikan tanggung jawab bagi mereka yang secara teknis mampu mengendalikan setiap penggunaan yang menyimpang dari yang diizinkan oleh hukum. Untuk alasan ini dan lainnya, tampaknya tindakan yang diambil oleh pihak berwenang sehubungan dengan penyedia ini tidak hanya diinginkan tetapi juga diperlukan untuk mencegah tindakan atau pelanggaran hukum apa pun selama komunikasi yang terjadi melalui infrastruktur penting ini. Khususnya, tidak ada kriteria yang jelas yang ditetapkan di tingkat internasional. Dalam hal ini, beberapa metode telah diusulkan di benua itu untuk menempatkan komunikasi di bawah pengawasan (setidaknya sebagian) dari lembaga-lembaga tersebut, yang masih didiskusikan dengan berbagai tingkat kesadaran dan partisipasi sosial.

10.2 PENYEDIA LAYANAN-ARTI DAN DEFINISI

Penyelenggara Layanan Jaringan adalah setiap orang yang menyediakan akses layanan informasi dalam bentuk elektronik. Mereka adalah entitas yang menyediakan pelanggan individu dan institusional dengan akses ke Internet. Bagian 79 dari Undang-Undang Teknologi Informasi, 2000 (I.T. Act, 2000) mengatur tanggung jawab Penyedia Layanan Jaringan. Penjelasan pada bagian ini menyatakan bahwa 'Penyedia Layanan Jaringan' berarti 'Perantara'. Menurut Bagian 2 (w) 'Perantara', sehubungan dengan pesan elektronik tertentu "berarti setiap orang yang atas nama orang lain menerima, menyimpan, atau mentransmisikan pesan itu atau menyediakan layanan apa pun sehubungan dengan pesan itu." Melihat definisi, tampak bahwa setiap orang yang memberikan layanan apa pun sehubungan dengan pesan elektronik termasuk menerima, menyimpan, mengirimkannya akan memenuhi syarat sebagai Perantara. Karena penerimaan dan pengiriman termasuk konektivitas, setiap orang yang menyediakan konektivitas seperti ISP atau Warnet juga termasuk dalam definisi Perantara ini. Namun bukan berarti semua perantara adalah ISP. Untuk misalnya mesin pencari seperti google.com bukanlah ISP.

Bagian 79 dari Undang-undang memberikan kekebalan kepada ISP dalam kasus kesalahan internet tertentu bahkan jika dilakukan melalui jaringan mereka asalkan mereka mengikuti pedoman uji tuntas, yang ditentukan secara rinci dalam Aturan Teknologi Informasi (Pedoman Perantara), 2011 dan dengan segera menghapus/menonaktifkan akses dalam hal mengetahui tindakan yang melanggar hukum atau menerima pemberitahuan pemerintah tentang hal itu. Kekebalan dari tanggung jawab ini, bagaimanapun, tidak berlaku ketika tindakan melanggar hukum menyangkut pelanggaran hak cipta atau paten, yang keduanya secara khusus dikecualikan dengan ketentuan pasal 81 Undang-Undang. Mengingat internet menjadi salah satu media utama untuk mengakses, mendistribusikan, dan yang paling penting melanggar konten berhak cipta, tanggung jawab ISP dalam kasus pelanggaran hak cipta ditetapkan oleh Undang-Undang Hak Cipta, 1957 sebagian besar berdasarkan Bagian 51(a) (ii) Undang-Undang yang, antara lain, menyatakan, setiap orang yang menyediakan "setiap tempat" untuk komunikasi pekerjaan yang melanggar, untuk keuntungan, kepada publik, bertanggung jawab atas pelanggaran kecuali dia dapat membuktikan bahwa dia tidak sadar atau dia tidak memiliki alasan yang masuk akal untuk mempercayai komunikasi tersebut kepada melanggar.

10.3 PENYEDIA LAYANAN-TANTANGAN GLOBAL

Mungkin tantangan terbesar bagi pembuat kebijakan nasional yang berurusan dengan Internet berasal dari konvergensi yang dibawa oleh Internet. Masalah yang berkaitan dengan ekonomi Internet tentu melibatkan masukan dari departemen perdagangan, media penyiaran, media cetak, telekomunikasi, elektronik, informasi, pendidikan, infrastruktur, tenaga kerja, dan keamanan nasional. Menyatukan departemen yang beragam ini dan menemukan keahlian kebijakan Internet domestik dari akademisi atau industri merupakan tantangan besar, terutama bagi negara berkembang yang agak lambat dalam menanggapi tantangan globalisasi dan media baru. Peraturan yang mengatur Internet sebagai media dan sebagai infrastruktur jatuh ke dalam tujuh kategori berikut: protokol dasar, infrastruktur

penyedia layanan Internet (ISP), konten, perilaku pengguna, e-commerce, akses universal, dan layanan nasional/pemerintah.

10.4 PENYEDIA LAYANAN-PERSPEKTIF INDIA

Frasa "setiap tempat" telah ditafsirkan untuk memasukkan ruang web oleh pengadilan menjadikan ISP sebagai pihak yang tepat dan diperlukan dalam setiap pelanggaran hak cipta di internet. Bahkan dalam salah satu perintah Pengadilan Tinggi Madras (RK Productions v. BSNL, Pengadilan Tinggi Madras, Gugatan Perdata 208/2012, O.A No. 230 Tahun 2012) melanjutkan dengan menyarankan bahwa tanpa ISP tidak akan ada pembajakan di internet. Yah, benar tetapi tidak akan ada akses internet juga. Hon'ble Court lebih lanjut menyatakan bahwa sejak di bawah UU IT; ISP memiliki kekuatan untuk memblokir situs web apa pun; itu bagi mereka untuk memastikan bahwa konten ilegal atau tidak bermoral tidak tersedia yang menyiratkan, sedikit keliru, bahwa adalah kekuatan ISP yang membuat mereka bertanggung jawab atas pelanggaran hak cipta.

Untuk memberikan bantuan kepada ISP, amandemen Undang-Undang Hak Cipta tahun 2012 memperkenalkan ketentuan pelabuhan aman tertentu tetapi tidak berhasil. Dalam perintah baru-baru ini oleh Pengadilan Tinggi Delhi di Star India Pvt. Ltd v. Haneeth Ujwal (Star India Pvt. Ltd v. Haneeth Ujwal, Pengadilan Tinggi Delhi, CS(OS) 2243/2014), menyatakan bahwa ISP memiliki kewajiban untuk memastikan bahwa tidak ada pelanggaran hak kekayaan intelektual pihak ketiga yang terjadi melalui jaringannya. Pengadilan meminta Perjanjian Lisensi antara Departemen Telekomunikasi dan ISP untuk membebani ISP dengan tanggung jawab untuk memastikan bahwa pekerjaan yang melanggar tidak dilakukan di jaringannya. Menariknya tidak disebutkan tentang ketentuan pelabuhan aman yang baru-baru ini diperkenalkan.

Peradilan India tampaknya mengalihkan beban mengidentifikasi pelanggaran pada ISP yang pada dasarnya merupakan kewajiban pemilik hak cipta mengabaikan fakta bahwa ISP tidak memiliki kapasitas kelembagaan dan logistik untuk mengasimilasi informasi pelanggaran di jutaan URL yang dapat diakses melalui jaringan mereka . Bahkan dalam (Kamlesh Vaswani v. Union of India KamleshVaswani v. Union of India, Supreme Court of India,Writ Petition (Civil) No(s). 177 tahun 2013), PIL diajukan ke Mahkamah Agung India pada tahun 2013, mencari larangan menyeluruh terhadap pornografi online , ISPAI (Asosiasi Penyedia Layanan Internet India) membuat pernyataan tegas di hadapan Pengadilan Tinggi bahwa tanpa dukungan hukum yang memadai dari pemerintah atau pengadilan, ISP tidak dapat melarang situs web. Meskipun masalah tersebut tidak melibatkan pelanggaran hak cipta, namun, argumen ISP bahwa "mereka tidak dapat dimintai pertanggungjawaban atas apa yang dilakukan orang di jaringan mereka seperti halnya perusahaan telekomunikasi tidak bertanggung jawab atas percakapan orang" tampaknya beralasan dan dapat diterapkan bahkan dalam beberapa kasus. di mana mereka tidak hanya bertanggung jawab atas pelanggaran hak cipta tetapi juga berkewajiban untuk mengidentifikasinya.

Mengapa Tidak Memadai?: Bagaimana jika ISP benar-benar mulai mengikuti mandat peraturan dan mulai memblokir situs web sesuai keinginan mereka. Tentu saja pemilik situs web dapat mendekati pengadilan, berpendapat bahwa kebebasan berbicara dan litigasi dapat berjalan dengan bahagia selamanya. Tetapi bagaimana jika situs web adalah perusahaan

rintisan kecil, berhati-hati untuk terlibat dalam litigasi yang mahal? Siapa yang kemudian akan memperbaiki ekses penyensoran online di mana ISP memiliki keleluasaan yang tidak terbatas dalam memutuskan kepada siapa mereka menyediakan akses? Meskipun dalam semua perintah yang dibahas di atas, peradilan telah mengamanatkan ISP untuk memastikan tidak ada pembajakan online, tidak ada pedoman untuk menyarankan situs web mana yang harus dilarang, hanya URL yang melanggar (Uniform Resource Locators) yang diblokir atau situs web lengkap, bagaimana dengan satu kali pelanggaran dan apakah mereka juga menjamin larangan total dan dalam kasus larangan - siapa yang memeriksa legalitasnya dan hak apa yang tersedia untuk pemilik situs web? Dan bagaimana jika ISP ini, didorong oleh kekuatan yang tak terkendali, juga mulai membedakan berbagai jenis konten, memberikan akses preferensial ke beberapa penyedia konten online atas yang lain sesuai minat mereka dan bukan pilihan konsumen? Mengingat bahwa India tidak memiliki undang-undang yang mewajibkan netralitas bersih bagi ISP, itu memang suatu kemungkinan.

Misalnya Bharti Airtel, ISP terkemuka di India, pada tahun 2013 telah bekerja sama dengan Google untuk menyediakan layanan data gratis hingga 1GB untuk mengakses mesin pencari Google, Gmail, dan layanan Google+ lainnya. Mempertimbangkan bahwa ISP mengeluarkan banyak pengeluaran untuk menyediakan infrastruktur bandwidth yang efisien ke situs web yang menginginkan akses lebih cepat, mereka mungkin ingin memulihkannya dengan membebankan tarif yang lebih tinggi dari mereka. Tetapi apakah diskriminasi antara konten semacam itu dapat dibenarkan? Bukankah itu akan merusak keterbukaan internet yang dikenal. Dan kalaupun dibiarkan sampai batas tertentu, tentu perlu diatur. Tetapi netralitas bersih belum ditangani oleh kerangka peraturan India yang menunjukkan dengan jelas kesenjangan peraturan. Sementara itu, masih harus dilihat kapan India akan menghilangkan kontras ironis dengan memiliki undang-undang yang berat namun tidak memadai.

10.5 ASOSIASI PENYEDIA LAYANAN INTERNET INDIA

Asosiasi Penyedia Layanan Internet India (ISPAI) didirikan pada tahun 1998 dengan misi untuk 'Mempromosikan Internet untuk kepentingan semua'. ISPAI adalah suara kolektif dari persaudaraan ISP dan dengan perluasan seluruh komunitas Internet. Selama bertahun-tahun ISPAI telah membantu mempengaruhi, membentuk dan membentuk kebijakan telekomunikasi, sehingga ISP dan pengusaha dalam bisnis Internet dapat mengatur dan mengembangkan layanan mereka dalam lingkungan yang mendukung dan memungkinkan. Dalam 10 tahun terakhir keberadaannya, telah menjadi pihak untuk mendobrak struktur monopoli di telekomunikasi, menurunkan hambatan masuk bagi ISP. Ini membantu membentuk India dari negara yang haus bandwidth menjadi negara surplus bandwidth. itu adalah semangat kompetitif dari anggota ISP ISPAI bahwa, akses Internet menjadi begitu luas dan hemat biaya tersedia untuk bangsa kita. ISP ini membantu menghubungkan India ke seluruh dunia dengan sangat efektif sehingga saat ini BPO dan Call Center tidak dapat tidak membuat kehadiran global mereka terasa berdasarkan konektivitas IP. India saat ini bisa dibilang di antara 10 negara teratas di dunia dalam hal jumlah pengguna Internet.

Hari ini ISPAI adalah badan puncak yang diakui dari ISP India di seluruh dunia. ISPAI memiliki akses dan sering berinteraksi dengan badan dan platform internasional dan sering

dikonsultasikan oleh mereka tentang langkah-langkah untuk tren masa depan dan pertumbuhan Internet. Ia bekerja sama dengan Pemerintah, Regulator serta Kamar Industri utama. Ini mendukung pertukaran delegasi, pengunjung bisnis dari seluruh dunia yang memberikan kesempatan kepada anggota ISP untuk berjejaring secara luas dan mencari peluang di tempat lain juga.

Ini adalah platform bagi komunitas Penyedia Solusi seperti produsen dan pemasok Perangkat Keras dan Perangkat Lunak untuk mendapatkan akses mudah ke klien ISP mereka, mempromosikan produk dan layanan mereka melalui pertemuan pribadi dan melalui acara yang didukung atau disponsori oleh ISPAI.

Kode Etik Penyedia Layanan Internet:

1. Maju

Mulai sejak tahun 1998, Pengguna Internet di negara kita telah tumbuh pada tingkat fenomenal lebih dari 200% per tahun, dan tren ini kemungkinan akan berlanjut selama bertahun-tahun yang akan datang. Diperkirakan bahwa pada 3 Maret akan ada sekitar 30 juta Pengguna Internet di Negara kita dan akan mencapai angka 100 juta pada tahun 2008. Dengan demikian Internet telah menjadi infrastruktur penting yang mendukung komunitas peneliti, sarjana, dan multi-disiplin yang tersebar luas. , pengusaha, profesional, pelajar bahkan rumah tangga. Seperti halnya infrastruktur umum lainnya (misalnya jalan, saluran air, pembangkit/distribusi listrik, dll), ada ketergantungan luas pada Internet oleh penggunanya untuk mendukung aktivitas sehari-hari. Pengoperasian Internet yang andal dan penggunaan sumber dayanya secara bertanggung jawab merupakan kepentingan dan perhatian bersama Pengguna, Operator, Sponsor, dan Masyarakat pada umumnya. Oleh karena itu, penting bagi Penyedia Layanan Internet untuk memahami tanggung jawab mereka dalam hal ini dan mengikuti praktik regulasi mandiri yang sehat. Kode Etik yang ditetapkan dalam dokumen ini adalah tanggapan sukarela dari Asosiasi Penyedia Layanan Internet India (ISPAI) terhadap persyaratan yang sah dari Masyarakat kita.

2. Pembukaan

2.1 Kode Etik ini terbuka untuk penerimaan sukarela oleh semua Anggota Asosiasi Penyedia Layanan Internet India (ISPAI).

2.2 Anggota ISPAI setuju bahwa mereka akan mematuhi Kode Etik ini secara tersurat dan tersurat.

2.3 Anggota ISPAI memahami bahwa kepatuhan terhadap Kode Etik ini tidak selalu berarti bahwa mereka bertindak sesuai dengan hukum. Referensi apa pun dalam Kode Etik tentang keabsahan atau pelanggaran hukum hanya terkait dengan Kerangka Hukum India.

2.4 Kode Etik ini dikeluarkan oleh Dewan Eksekutif ISPAI, yaitu: satu-satunya kewenangan untuk mengubahnya dari waktu ke waktu sesuai dengan Peraturan & Ketentuan ISPAI.

3. Tujuan

3.1. Tujuan Kode Etik ISPAI adalah untuk menyatakan dan mempertahankan standar yang tinggi dari Praktik Etika dan Profesional di bidang Layanan Internet.

4. Prinsip

4.1 Dalam upaya mencapai tujuannya, Kode Etik ISPAI didasarkan pada Prinsip-prinsip berikut:

* Teknologi netral;

• Adil bagi semua pihak;

• Perlindungan Data Pengguna;
• Tanggung jawab atas konten di Internet berada pada Penyedia Konten yang relevan.

5. Praktek Wajib

5.1 Kewajiban Hukum

5.1.1 ISPAI dan Anggotanya memiliki tanggung jawab untuk mematuhi hukum dan bekerja sama dengan Lembaga Penegakan Hukum yang bertindak dalam Kerangka Hukum India yang ditentukan.

5.1.2 Anggota tidak akan dengan sengaja mengizinkan Pengguna atau sesama Anggota untuk terlibat dalam aktivitas ilegal apa pun dalam hal ketentuan Undang-Undang Teknologi Informasi 2000, Kebijakan ISP dan kerangka hukum lain yang berlaku.

5.1.3 Anggota akan mengikuti dan mematuhi semua hukum yurisdiksi yang berkaitan dengan pelaporan transaksi.

5.1.4 Anggota, Layanan dan Materi Promosi mereka tidak akan mendorong sesuatu secara terang-terangan, yang dengan cara apapun melanggar hukum.

5.2 Kewajiban kepada Publik

5.2.1 Anggota akan berurusan secara adil dengan sesama profesional dan publik, dengan menghormati hak dan kepentingan sah orang lain.

5.2.2 Anggota akan berusaha untuk mendukung Prakarsa Pelayanan Publik secara harmonis dengan yurisdiksi di mana mereka menyediakan Layanan mereka.

5.2.3 Anggota akan memastikan bahwa Layanan dan Materi Promosi mereka tidak berisi apa pun, yang dapat memicu kekerasan, kekejaman atau kebencian atas dasar diskriminasi seksual, pemeran, keyakinan atau agama.

5.2.3 Anggota harus memastikan bahwa anak di bawah umur tidak didaftarkan oleh mereka untuk Internet Layanan kecuali dengan izin eksplisit dari orang tua/wali mereka.

5.3. Kewajiban Memiliki Profesi

5.3.1 Anggota akan mematuhi semua Syarat & Ketentuan Perjanjian Lisensi dalam surat dan semangat Untuk Penyediaan Layanan Internet.

5.3.2 Anggota harus jujur dalam semua kegiatan promosi dan mempublikasikannya informasi yang tanpa ketidakakuratan, ambiguitas, berlebihan atau kelalaian tentang operasi mereka, layanan dan harga kepada Pelanggan dan Instansi Pemerintah / Swasta.

5.3.3 Anggota akan melembagakan kontrol untuk mendeteksi dan menghilangkan penipuan dan melindungi data mereka dan sistem dari pelanggaran internal dan eksternal.

5.3.4 Anggota akan bekerja sama satu sama lain dalam menyelidiki dan mencegah kasus Peretasan. .

5.3.5 Anggota akan melembagakan tindakan pengendalian yang memadai untuk mencegah akses tidak sah ke sumber daya Layanan Internet.

5.3.6 Anggota harus memastikan bahwa mereka secara eksplisit memberitahukan tentang pelanggan, semua Syarat dan Ketentuan untuk penyediaan Layanan mereka, sebelum pelanggan tersebut mendaftar dengan Anggota untuk Layanan mereka.

5.4 Kewajiban kepada Pelanggan

5.4.1. Anggota memiliki tanggung jawab untuk menjelaskan Kode Etik ini kepada semua Klien mereka serta Mitra Penyalur/Distributor mereka dan menunjukkan kepada mereka bahwa setiap pelanggaran Kode Etik dan/atau pelanggaran hukum akan mengakibatkan penghentian layanan.

5.4.2 Anggota akan merancang dan mengoperasikan Layanan mereka untuk memberikan

privasi dan kerahasiaan dan akan memposting praktik dan prosedur kerahasiaan mereka dengan tepat.

5.4.3 Anggota akan mengikuti praktik industri terbaik dalam menawarkan Pelanggan terbaru

Memfilter Perangkat Lunak dan memberi tahu mereka tentang perangkat lunak apa pun, yang dapat mereka gunakan untuk melindungi data rahasia dan privasi mereka.

5.4.4 Anggota akan mengikuti praktik industri terbaik dalam menggunakan Anti-Spamming Perangkat Lunak, sehingga Pelanggan dapat memilih untuk meminimalkan jumlah Spam yang dikirim ke akun email mereka.

5.4.5 Dimana Layanan Internet melibatkan pengumpulan informasi pribadi seperti: nomor telepon, rincian kartu kredit dan alamat dll dari pelanggan, Anggota wajib menjelaskan kepada mereka tujuan penggunaan informasi tersebut.

6. Keluhan

6.1 Karena Kode Etik ini terbuka untuk penerimaan sukarela oleh semua Anggota ISPAI, Dewan Eksekutif menganggap bijaksana untuk tidak melembagakan Prosedur Penanganan Keluhan pada tahap awal. Namun, situasi ini dapat ditinjau kemudian.

10.6 TEKNOLOGI AKSES INTERNASIONAL

Sambungan antara perangkat berkemampuan Internet Anda dan jaringan global dijalankan melalui teknologi transmisi data digital tertentu. Ini mewakili transfer paket informasi melalui rute Protokol Internet. Menurut metode transmisi data, akses Internet yang diberikan ISP kepada pengguna dapat dibagi menjadi beberapa jenis, yang paling populer di antaranya adalah:

Akses Internet dial-up

Ini adalah metode tertua untuk menyediakan akses ke Internet. Ini menggunakan saluran telepon untuk melakukan koneksi modem-ke-modem. Untuk tujuan itu, komputer pengguna disambungkan ke perangkat modem berkemampuan saluran telepon, yang menghubungi simpul ISP dan mulai mentransfer data antara server yang menyimpan situs web yang ingin dilihat pengguna dan perangkat mereka yang terhubung ke Internet. Internet dial-up saat ini dianggap ketinggalan zaman di sebagian besar masyarakat Internet karena kecepatan koneksi yang lambat (sekitar 40-50 kbit/s.). Namun, ketersediaan akses telepon yang luas membuat akses Internet jenis ini menjadi satu-satunya alternatif untuk daerah terpencil yang tetap berada di luar jaringan broadband. Ini juga merupakan layanan akses Internet paling murah dan lebih disukai oleh pengguna dengan anggaran terbatas.

DSL

DSL, kependekan dari 'digital subscriber loop' atau 'digital subscriber line', adalah versi lanjutan dari metode akses Internet dial-up. Berbeda dengan dial-up, DSL menggunakan frekuensi tinggi untuk melakukan koneksi melalui jaringan telepon lokal. Hal ini memungkinkan Internet dan sambungan telepon dijalankan pada satu saluran telepon yang sama. Teknologi saluran pelanggan digital memastikan Asymmetric Digital Subscriber Line (ADSL), di mana kecepatan upload lebih rendah dari kecepatan download, dan Symmetric Digital Subscriber Line (SDSL), menawarkan kecepatan upload dan download yang sama. Dari keduanya, ADSL jauh lebih populer dan bahkan dikenal hanya sebagai DSL bagi pengguna.

Internet kabel

Internet kabel adalah salah satu metode yang paling disukai untuk menyediakan akses Internet perumahan. Secara teknis, ini merupakan metode akses Internet broadband, menggunakan jaringan televisi kabel bandwidth tinggi untuk mengirimkan data antara jaringan global dan rumah tangga. Untuk menggunakan Internet kabel, Anda memerlukan modem kabel di rumah yang akan terhubung dengan CMTS (Cable Modem Termination System) dari ISP kabel Anda. Akses Internet kabel dapat ditawarkan bersama-sama dengan berlangganan televisi kabel dan secara terpisah, untuk kenyamanan pelanggan. Kasus kedua menimbulkan biaya berlangganan yang lebih tinggi karena biaya pemasangan peralatan tambahan.

Pita Lebar Nirkabel (WiBB)

Ini adalah teknologi akses Internet broadband generasi baru, yang memungkinkan pengiriman Internet nirkabel berkecepatan tinggi dalam area yang luas. ISP broadband nirkabel (WISP) memastikan kecepatan koneksi yang mendekati kecepatan broadband kabel yang disediakan oleh DSL dan ISP kabel. Untuk mendapatkan broadband nirkabel, Anda perlu menempatkan antena khusus di atap rumah atau balkon apartemen Anda dan mengarahkannya ke pemancar WISP Anda. Jenis akses Internet ini digunakan sebagai alternatif koneksi broadband kabel di daerah terpencil.

Internet Wi-Fi

Wi-Fi (dari Wireless Fidelity) telah menjadi salah satu metode akses Internet yang paling banyak didistribusikan, dengan meningkatnya penggunaan komputer portabel dan perangkat seluler berkemampuan Internet, seperti ponsel pintar, PDA, konsol game, dll. adalah metode akses Internet yang paling mobile, karena Anda dapat menggunakannya di mana saja selama Anda berada dalam cakupan jangkauan, yaitu dalam jangkauan jaringan nirkabel yang terhubung ke Internet. Karena kemampuannya untuk melayani perangkat seluler, Wi-Fi digunakan di tempat-tempat umum seperti bandara, hotel, dan restoran untuk menyediakan akses Internet kepada pelanggan. Ada juga hotspot Wi-Fi khusus di mana layanannya gratis atau berbayar. Beberapa kota terbesar di dunia sedang dalam proses membangun jaringan Wi-Fi yang mencakup semua tempat umum di area pusat.

ISDN

Metode transmisi data online lain yang layak dipertimbangkan adalah ISDN atau Integrated Services Digital Network. ISDN mewakili jaringan sistem telepon, yang mengintegrasikan transmisi suara dan data digital berkualitas tinggi melalui saluran telepon biasa. Memastikan transmisi data yang jauh lebih baik melalui saluran telepon daripada yang dimungkinkan oleh saluran analog, ISDN menawarkan kecepatan koneksi Internet hulu/hilir

yang cepat 128 kbit/dtk. Tingkat kecepatan ini dapat dianggap sebagai kecepatan broadband sebagai lawan dari kecepatan narrowband dari saluran telepon analog standar 56k.

Ethernet

Jenis akses Internet lain yang layak disebut adalah Ethernet - teknologi LAN kabel (jaringan area lokal) yang paling tersebar luas, juga digunakan dalam LAN nirkabel. Teknologi Ethernet dapat memastikan berbagai tingkat kecepatan dan dengan demikian dapat dibagi menjadi beberapa jenis: Ethernet biasa, menyediakan kecepatan transmisi hingga 10 mbit/s, Ethernet cepat, menawarkan hingga 100 mbit/s, gigabit Ethernet, mendukung 1 gbit/s dan Ethernet 10-Gbit, dengan kecepatan hingga 10 gbit/s.

10.7 AKUNTABILITAS DAN KEWAJIBAN PENYEDIA LAYANAN

Ketika internet pertama kali menjadi populer di tahun 1990-an, pembuat konten menjadi semakin khawatir bahwa pekerjaan mereka akan ditempatkan secara online dan didistribusikan tanpa persetujuan mereka (dan tanpa pengembalian investasi mereka). Di dunia nyata, ada biaya fisik dan investasi waktu yang harus dikeluarkan untuk menyalin sesuatu seperti CD, dan biaya itu ditanggung untuk setiap CD yang dibuat. Konten digital di sisi lain memiliki biaya "menyalin" hampir nol karena setelah salinan awal dibuat, jutaan salinan dapat dibuat tanpa biaya tambahan - seringkali hanya dengan mengklik tombol.

Oleh karena itu, penyedia konten mengambil sikap bahwa ISP serupa dengan majalah dan surat kabar dan harus bertanggung jawab atas materi yang "diterbitkan" atau diizinkan untuk diterbitkan. ISP berpendapat bahwa mereka lebih mirip dengan perusahaan telepon, dan benar-benar hanya media untuk berkomunikasi dan tidak harus bertanggung jawab atas segala sesuatu yang melewati sistem mereka.

Pada akhirnya, Kongres masuk dan mengesahkan serangkaian undang-undang termasuk Digital Millennium Copyright Act (DMCA), yang memihak ISP, tetapi juga menerapkan perlindungan untuk menenangkan penyedia konten.

ISP dapat dimintai pertanggungjawaban atas pelanggaran hak cipta penggunanya, tetapi hanya dalam keadaan yang sangat terbatas. Secara umum, ada tiga cara ISP dapat bertanggung jawab atas pelanggaran hak cipta, yaitu:

- Pelanggaran langsung : pelanggaran langsung adalah jika ISP secara sadar meng-host materi berhak cipta dan menerima keuntungan finansial langsung darinya.
- Kewajiban perwakilan : ISP dapat bertanggung jawab secara perwakilan jika ISP memiliki hak dan kemampuan untuk mengontrol penggunanya dan menerima keuntungan finansial langsung dari pelanggaran hak cipta.
- Pelanggaran kontributif : ISP dapat bertanggung jawab berdasarkan teori tanggung jawab "kontribusi" jika ISP mengetahui aktivitas yang melanggar dan memberikan kontribusi material (meskipun membantu) terhadap pelanggaran hak cipta.

Hampir semua kasus mengandalkan teori pelanggaran kontributif. Pelanggaran langsung hampir tidak pernah terjadi dan vicarious liability sulit dibuktikan karena perlu dibuktikan bahwa ISP memiliki hak dan kemampuan untuk mengendalikan pelanggannya. Meskipun mungkin sulit untuk menemukan bukti bahwa ini masalahnya, ISP tetap harus berhati-hati karena perjanjian persyaratan layanan mereka dapat menetapkan bahwa mereka memiliki hak dan kemampuan untuk mengontrol pelanggan mereka.

DMCA umumnya melindungi ISP dari kewajiban pelanggaran hak cipta di bawah ketentuan "pelabuhan aman". Agar memenuhi syarat untuk perlindungan safe harbour, ISP harus:

- Tidak memiliki pengetahuan yang sebenarnya tentang pelanggaran hak cipta;
- Tidak mendapat keuntungan finansial dari pelanggaran tersebut;
- Mematuhi ketentuan "pemberitahuan" atau "penghapusan" apa pun untuk menghapus materi hak cipta; dan
- Membentuk agen untuk menangani keluhan pelanggaran hak cipta

Misalnya, sebuah perusahaan rekaman bernama UberStars mengetahui bahwa CD oleh salah satu artis rekamannya telah diposting di situs web yang dihosting oleh ISP bernama MegaNet. Untuk menghindari tanggung jawab, MegaNet harus tidak mengetahui materi yang melanggar dan telah membentuk agen yang dapat dihubungi UberStars dengan pemberitahuan penghapusan.

Setelah UberStars mengirimkan pemberitahuan penghapusan, MegaNet harus secara fisik menghapus materi yang melanggar atau menonaktifkan akun dan akses pengguna yang melanggar. Jika MegaNet gagal menunjuk agen untuk dihubungi atau mengambil langkah yang diperlukan setelah menerima pemberitahuan penghapusan, maka UberStars dapat menuntut MegaNet, dan MegaNet tidak dapat menggunakan DMCA untuk menghindari tanggung jawab. Selama tahun 1990-an seiring dengan semakin populernya internet, semakin banyak orang beralih ke internet sebagai sumber berita dan informasi yang mau tidak mau mengarah pada kasus pencemaran nama baik online pertama. Dalam salah satu kasus besar pertama, Drudge Report, sebuah situs online yang menawarkan berita politik dan gosip, menyatakan bahwa seorang pembantu Presiden Clinton memiliki sejarah pelecehan pasangan. Ajudan tersebut kemudian mengajukan gugatan pencemaran nama baik terhadap Laporan Kerja Keras serta ISP yang menampungnya, AOL.

Jika pengadilan memperlakukan AOL sebagai surat kabar atau majalah tradisional, maka pengadilan akan bertanggung jawab atas cedera yang disebabkan oleh pernyataan palsu Drudge Report. Sebaliknya, pengadilan menemukan bahwa, karena AOL adalah ISP, itu dilindungi oleh Bagian 230 dari Communications Decent Act (CDA). CDA secara eksplisit menyatakan bahwa tidak ada ISP "yang akan diperlakukan sebagai penerbit atau pembicara dari setiap informasi yang diberikan oleh penyedia konten informasi lain." Ini menetapkan preseden bahwa ISP tidak seperti surat kabar dan majalah dan dilindungi di bawah CDA untuk tanggung jawab berdasarkan pernyataan online penggunanya, termasuk pencemaran nama baik dan kecabulan.

Meskipun ISP umumnya dilindungi di AS, ini tidak selalu benar di luar negeri. Perilaku yang sama yang dilindungi ISP di AS telah dituntut di negara-negara seperti Inggris dan Jerman. Misalnya, AOL telah dituntut karena menjadi tuan rumah komentar yang memfitnah di Inggris dan telah dituntut karena menampung materi yang melanggar di Jerman. Setiap negara memiliki undang-undangnya sendiri, dan undang-undang ini sangat bervariasi dari satu negara ke negara lain. Oleh karena itu, karena jangkauan internet bersifat internasional, sangat penting untuk mengetahui secara pasti apa yang dilindungi dan apa yang tidak dilindungi di negara tempat Anda mengharapkan orang untuk melihat konten Anda.

10.8 JENIS DAN KATEGORI PENYEDIA LAYANAN

Penyedia Layanan Internet (ISP), yang pertama kali muncul pada akhir 1980-an dan awal 1990-an, adalah bisnis dan organisasi yang menyediakan akses Internet dan layanan terkait kepada pengguna. Penyedia ini menghubungkan pelanggan ke pelanggan penyedia layanan lain melalui jaringan. Seringkali, Penyedia Layanan Internet (juga disebut Penyedia Akses Internet) adalah perusahaan yang menyediakan layanan telekomunikasi termasuk akses komunikasi data dan koneksi telepon. Mayoritas perusahaan telepon sekarang berfungsi sebagai Penyedia Akses Internet juga. ISP mungkin komersial, nirlaba, milik pribadi atau milik komunitas. Ada beberapa jenis Penyedia Layanan Internet yang tersedia saat ini, termasuk akses, kotak surat, hosting, transit, virtual, dan gratis.

Akses ISP — Menggunakan berbagai teknologi untuk memfasilitasi koneksi konsumen ke jaringan mereka. Teknologi ini mungkin termasuk broadband atau dialup. Jenis koneksi broadband yang selalu aktif terdiri dari kabel, layanan serat optik (FiOS), DSL (Digital Subscriber Line), dan satelit. Sejumlah penyedia akses juga menyediakan layanan email dan hosting.

ISP kotak surat — Menawarkan layanan hosting kotak surat email dan server email untuk mengirim, menerima, dan menyimpan email. Banyak ISP kotak surat juga merupakan penyedia akses.

Hosting ISP — Menawarkan email, File Transfer Protocol (FTP), layanan hosting web, mesin virtual, cloud, dan server fisik.

ISP Transit — Menyediakan bandwidth dalam jumlah besar yang diperlukan untuk menghubungkan ISP hosting dan mengakses ISP secara bersamaan.

ISP Virtual (VISP) — Membeli layanan dari ISP lain untuk memungkinkan pelanggan mengakses Internet.

ISP Gratis (freenets) – Menyediakan layanan gratis dan sering menampilkan iklan saat pengguna terhubung.

Untuk menghubungkan komputer Anda ke Internet, Anda memerlukan Internet Service Provider (ISP). Beberapa perusahaan membatasi layanan mereka untuk menyediakan akses Internet saja. Lainnya, seperti perusahaan telepon atau kabel, mungkin menawarkan akses Internet sebagai bagian dari paket layanan yang lebih besar. Pertimbangkan faktor-faktor ini saat memilih penyedia:

- Kecepatan. Jika Anda hanya ingin memeriksa email dan membaca halaman web, koneksi dial-up mungkin sudah cukup. Namun jika Anda ingin mengunduh musik atau acara televisi atau menonton video, Anda memerlukan koneksi yang lebih cepat dengan akses broadband, seperti digital subscriber line (DSL), modem kabel, atau satelit.
- Ketersediaan: Perusahaan mana yang menawarkan layanan di wilayah Anda?
- Akses nirkabel: Bisakah Anda mendapatkan koneksi nirkabel untuk komputer lain di rumah Anda?
- E-mail: Apakah akun e-mail disertakan dengan layanan ini? Berapa batas penyimpanan di kotak surat Anda?
- Perangkat Lunak: Apakah ada perangkat lunak yang diperlukan untuk mengaktifkan layanan?

- Dukungan: Jenis dukungan apa yang tersedia: telepon, email, obrolan, dll.? Apakah dukungannya gratis?
- Fitur Khusus: Layanan apa yang disediakan untuk pemblokiran spam, perlindungan virus, pesan instan, dan ruang obrolan?
- Persyaratan Layanan: Apakah ada batasan jumlah data yang dapat Anda gunakan per bulan?
- Biaya: Berapa biaya bulanan untuk layanan ini? Apakah ada biaya untuk menyewa modem atau memasangnya?

10.9 STUDI KASUS

Peraturan Perantara Hak Asasi Manusia dan Internet di Chili: Pada tanggal 4 Mei 2010, Kongres Chili mengadopsi undang-undang baru yang mengatur pertanggungjawaban perantara Internet untuk penegakan hak cipta online di bawah Perjanjian Perdagangan Bebas Chili – AS tahun 2004. Undang-undang mengharuskan perintah pengadilan sebelum Penyedia Layanan Internet diharuskan untuk menghapus materi yang diduga melanggar hak cipta dari situs web, mengungkapkan informasi pelanggan, atau menghentikan akun Internet pelanggan.

Bab III Undang-Undang Kekayaan Intelektual (Pasal 85L-85U) menyediakan satu set pelabuhan untuk penyedia layanan jaringan. [LINK ke halaman Chili] Jika penyedia layanan Internet mematuhi ketentuan yang ditetapkan dalam undang-undang, mereka dibebaskan dari sanksi keuangan yang timbul dari klaim pelanggaran hak cipta. Namun, perantara Internet masih tunduk pada perintah, dan tindakan hukum wajar lainnya yang ditujukan untuk memblokir akses online ke konten tertentu yang diduga melanggar hak cipta.

Undang-undang ISP Chili memiliki fitur unik yang membedakannya dari kerangka peraturan serupa lainnya di negara lain. Pemberitahuan Chili dan prosedur mencatat tunduk pada tinjauan akhir oleh hakim, bukan diserahkan kepada kebijaksanaan individu ISP. Kerangka kerja ini didasarkan pada kewajiban hak asasi manusia Chili sebagai penandatangan Konvensi Amerika tentang Hak Asasi Manusia (kadang-kadang disebut sebagai Pakta San José), dan pada prinsip-prinsip dasar dalam Konstitusi Chili.

Dokumen ini menguraikan kewajiban hak asasi manusia internasional yang mendukung pendekatan tatanan yudisial terhadap peraturan perantara Internet yang diambil oleh pemerintah Chili. Kerangka kerja ini memiliki relevansi yang sama dengan negara-negara Amerika Latin lainnya yang menandatangani Konvensi Amerika tentang Hak Asasi Manusia, dan yang merupakan pihak dalam perjanjian perdagangan dengan AS, termasuk perjanjian bilateral (FTA Chili-AS, Peru-AS FTA, Kolombia – FTA AS, [Panama – U.S. FTA]), perjanjian regional (CAFTA-DR), atau perjanjian plurilateral (ACTA)); atau sedang dalam proses negosiasi perjanjian perdagangan dengan AS yang mencakup ketentuan tentang kewajiban ISP atas pelanggaran kekayaan intelektual (Perjanjian Kemitraan Trans-Pasifik).

Semua Perjanjian Perdagangan Bebas A.S. sejak tahun 2002 telah memasukkan ketentuan terperinci yang mengatur kewajiban ISP atas pelanggaran hak cipta di bagian penegakan bab tentang kekayaan intelektual. Ketentuan tersebut mengharuskan negara penandatangan untuk memberikan "insentif hukum bagi penyedia layanan untuk bekerja sama dengan pemilik hak cipta dalam menghalangi penyimpanan dan pengiriman materi

berhak cipta yang tidak sah" (apakah hukum nasional mitra dagang mengakui kewajiban sekunder atas pelanggaran hak cipta), dan untuk menetapkan pembatasan kewajiban ISP di mana ISP mematuhi ketentuan rinci yang ditetapkan dalam FTA.

Meskipun tidak ada kewajiban dalam perjanjian kekayaan intelektual internasional saat ini yang mengatur kewajiban penyedia layanan Internet atas pelanggaran hak cipta, FTA A.S. membingkai ketentuan ini sebagai persyaratan bagi negara-negara untuk menerapkan kewajiban mereka yang ada sebagai anggota Organisasi Perdagangan Dunia, di bawah Perjanjian 1994 tentang Perdagangan -Aspek Terkait Kekayaan Intelektual (TRIPs). Ketentuan dalam setiap perjanjian dimulai dengan kata-kata yang persis mencerminkan bahasa Pasal 41 TRIPs:

Untuk tujuan menyediakan prosedur penegakan yang memungkinkan tindakan efektif terhadap setiap tindakan pelanggaran hak cipta yang tercakup dalam Bab ini, termasuk pemulihan cepat untuk mencegah pelanggaran dan pemulihan pidana dan perdata, masing-masing Pihak harus menyediakan, sesuai dengan kerangka yang ditetapkan dalam Pasal ini.

Pasal 17.10.23 bab kekayaan intelektual dari FTA AS-Chili mewajibkan Chili dan AS untuk menyediakan tempat perlindungan yang aman terhadap tanggung jawab atas pelanggaran hak cipta untuk perantara Internet yang membuat salinan cache, menghosting konten atas permintaan pengguna, menawarkan layanan pencarian, dan menyediakan tautan dan alat lokasi lainnya, dengan syarat mereka menghapus konten yang diduga melanggar hak cipta setelah menerima pemberitahuan yang sah dari pemegang hak cipta.

Paragraf (f) Pasal itu menetapkan bahwa:

Untuk tujuan proses pemberitahuan dan penghapusan (...) masing-masing Pihak harus menetapkan prosedur yang sesuai melalui proses yang terbuka dan transparan yang ditetapkan dalam hukum domestik, untuk pemberitahuan efektif atas pelanggaran yang diklaim, dan pemberitahuan tanggapan yang efektif oleh mereka yang materinya dihapus atau dinonaktifkan karena kesalahan atau kesalahan identifikasi.

Dengan demikian, FTA AS-Chili memberi Chili dan AS fleksibilitas yang cukup besar dalam cara mereka menerapkan sistem pemberitahuan dan penghapusan. Persyaratan untuk "pemberitahuan efektif" dan "prosedur yang sesuai" tidak membatasi proses untuk pemberitahuan dari pihak swasta atau badan administratif. Mengingat bahwa pemberitahuan pihak swasta dan prosedur pencopotan berpotensi bertentangan dengan persyaratan untuk proses hukum dan perlindungan hukum hak asasi manusia warga negara yang dijamin dalam Konstitusi Chili dan ACHR, kesimpulan yang dibuat oleh Kongres Chili dan tercermin dalam Kekayaan Intelektual 2010 Undang-undang adalah bahwa ISP hanya akan diminta untuk menghapus konten yang diduga melanggar setelah menerima perintah dari hakim, setelah peninjauan kembali. .Kongres Chili percaya bahwa kerangka kerja ini akan memberikan perlindungan yang diperlukan untuk hak-hak dasar warga negara yang dijamin secara konstitusional, sambil menerapkan kewajiban Chili dalam Chili-U.S.FTA.

Bukan Hanya Chili - Relevansi untuk Negara Lain: Kerangka perlindungan konstitusional dan jaminan hak-hak dasar yang dijelaskan di atas berlaku sama untuk negara-negara Amerika Latin lainnya yang menandatangani Konvensi Amerika tentang Hak Asasi Manusia, dan negara-negara lain yang memiliki kewajiban serupa di bawah regional atau negara lain. instrumen internasional. Dengan demikian, pendekatan tatanan peradilan Chili untuk menerapkan

peraturan ISP mungkin juga tersedia untuk negara lain yang sedang mempertimbangkan mekanisme untuk menerapkan kewajiban penegakan kekayaan intelektual online dalam perjanjian bilateral, regional dan plurilateral dengan cara yang paling melindungi hak warga negara atas proses hukum, kebebasan ekspresi, dan privasi.

10.10 FORUM TATA KELOLA INTERNET REGIONAL ASIA PASIFIK

Saat ini, Asia memiliki permintaan alamat Internet yang tumbuh paling kuat. Artinya semakin banyak orang di Asia yang menggunakan Internet. Berbeda dengan Amerika Utara dan Eropa, permintaan Internet di Asia tidak hanya tumbuh, tetapi juga tumbuh dengan kecepatan yang semakin cepat. Forum Tata Kelola Internet Regional Asia Pasifik (APrIGF) berfungsi sebagai platform untuk diskusi, pertukaran dan kolaborasi di tingkat regional, dan juga jika memungkinkan untuk menggabungkan diskusi IGF nasional, yang pada akhirnya memajukan pengembangan tata kelola Internet di kawasan Asia Pasifik. Pada tahun 2010, sementara IGF global sudah memasuki tahun kelima dan terakhir dari piagam awalnya, dan IGF Regional telah didirikan di banyak kawasan lain, termasuk Afrika, Eropa, Amerika Latin dan Karibia, hingga saat ini, Asia belum melihat paralelnya. forum untuk membahas masalah tata kelola Internet di tingkat regional.

Oleh karena itu, untuk pertama kalinya, APRIGF diselenggarakan dengan tujuan untuk meningkatkan kesadaran dan mendorong partisipasi dari pemangku kepentingan terkait di seluruh kawasan tentang masalah tata kelola Internet, serta untuk mendorong diskusi multi-lateral dan multi-pemangku kepentingan tentang isu-isu yang berkaitan dengan Internet di Asia. Pendekatan multi-stakeholder adalah prinsip inti APRIGF dengan penekanan pada keragaman peserta dan keterbukaan diskusi. Menghargai kaum muda sebagai pemangku kepentingan penting dan generasi masa depan Internet, IGF Pemuda juga menjadi bagian integral dari APRIGF di mana mereka diadakan secara paralel setiap tahun yang menampilkan simulasi model diskusi multi-stakeholder di antara kaum muda di berbagai Internet masalah pemerintahan.

Apa itu Forum Tata Kelola Internet (IGF)?: Membangun Tujuan Pembangunan Milenium Perserikatan Bangsa-Bangsa (PBB), dan mandat yang diberikan pada Tahap Kedua KTT Dunia tentang Masyarakat Informasi di Tunis pada tahun 2005, IGF (Forum Tata Kelola Internet) adalah kegiatan Perserikatan Bangsa-Bangsa yang dimulai pada tahun 2006 sebagai platform global untuk dialog kebijakan multi-stakeholder tentang isu-isu yang ada dan muncul di tata kelola Internet untuk mendorong keberlanjutan, ketahanan, keamanan, stabilitas dan pengembangan Internet. Forum tahunan sebelumnya diadakan di Yunani (2006), Brasil (2007), India (2008), dan Mesir (2009), Lituania (2010), Kenya (2011), Azerbaijan (2012). Internet telah menjadi bagian integral dari kehidupan masyarakat. Terlepas dari keuntungannya, penyalahgunaan dan penyalahgunaan menyebabkan masalah sosial, seperti kesenjangan digital, kecanduan internet, keamanan informasi, keamanan, privasi, dan masalah lain yang berkembang. Isu-isu ini tidak menghormati batas-batas negara, dan oleh karena itu memerlukan kolaborasi antara negara dan wilayah untuk mengatasinya. Pendekatan IGF merupakan forum terbuka untuk berbagi pengetahuan antar pemangku kepentingan lintas batas, yang pada gilirannya menginformasikan pengembangan kebijakan lokal.

10.11 RINGKASAN

Penyedia Layanan Internet di seluruh dunia memiliki begitu banyak masalah dan tidak ada satu kerangka hukum di tingkat nasional dan nasional untuk menangani masalah sektor ini. Dalam unit ini konsep penyedia layanan-makna dan definisi, tantangan global sebelum penyedia layanan, penyedia layanan dalam perspektif India, Peran dan pentingnya Asosiasi Penyedia Layanan Internet India, teknologi akses internasional, aksesibilitas dan kewajiban penyedia layanan dan jenis & kategori penyedia layanan dibahas panjang lebar untuk pemahaman yang lebih baik dan kejelasan tentang intinya.

10.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Penulis)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang sesuai dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

10.13 PERIKSA KEMAJUAN ANDA

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a Munculnya bentuk-bentuk baru komunikasi massa melalui teknologi telah menimbulkan hambatan dan tantangan regulasi.
b Mesin pencari seperti google.com bukanlah Internet Service Provider (ISP).
c Ungkapan "setiap tempat" telah ditafsirkan untuk memasukkan ruang web oleh pengadilan.
d ISP memiliki kewajiban untuk memastikan bahwa tidak ada pelanggaran hak kekayaan intelektual pihak ketiga yang terjadi melalui jaringannya.
e DSL, singkatan dari 'digital subscriber loop' atau 'digital subscriber line', adalah versi lanjutan dari metode akses internet dial-up.

B. Isi Bagian yang Kosong:

i Penyedia Layanan Jaringan berarti setiap orang.....dalam bentuk elektronik.
ii ..... UU IT, 2000 terkait dengan tanggung jawab Penyedia Layanan Jaringan.
iii UU IT, 2000 memberikan kekebalan kepada ISP dalam kasus-kasus tertentu kesalahan internet bahkan jika itu dilakukan melalui jaringan mereka asalkan mereka mengikuti .....
iv Asosiasi Penyedia Layanan Internet India didirikan di.....dengan misi untuk "mempromosikan internet untuk manfaat semua".
v ..... telah menjadi salah satu metode akses internet yang paling banyak didistribusikan.

10.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Siapa yang menyediakan akses ke informasi
2. Bagian 79
3. Pedoman uji tuntas
4. 1998
5. WI-Fi (dari Wireless Fidelity)

10.15 PERTANYAAN TERMINAL

1. Apa pengertian dan definisi dari Penyedia Jasa?
2. Bagaimana posisi penyedia layanan dalam Perspektif India?
3. Tulis catatan di Asosiasi Penyedia Layanan Internet India.
4. Bagaimana pertanggungjawaban dan kewajiban penyedia jasa?
5. Membahas berbagai jenis dan kategori penyedia layanan.

BAB 11
PERLINDUNGAN KONTEN DI SITUS WEB

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami masalah dan pokok bahasan yang terkait dengan Perlindungan Konten di Situs Web
- Memahami konsep dengan mengacu pada penggunaan Konten Web
- Memahami masalah teknis dan hukum terkait Perlindungan Konten di Situs Web

11.1 PENGANTAR

Melindungi situs web Anda dari pencurian sekarang dianggap wajib bagi pemilik situs web. Ini sangat penting untuk situs web yang "berat konten" - gambar, grafik, video, dll. Sama seperti dunia "batu bata dan mortir", tidak ada jaminan 100% terhadap pencurian online tetapi ada banyak hal yang dapat Anda lakukan untuk melindungi diri Anda dan situs Anda. Kebanyakan pencurian online terjadi adalah karena “mudah” melakukannya. Sama seperti membiarkan pintu depan Anda terbuka atau mobil Anda tidak terkunci, jika Anda membuatnya mudah bagi pencuri, mereka akan memanfaatkannya.

11.2 KONTRAK SITUS WEB

Persyaratan penggunaan situs web atau perjanjian persyaratan layanan merupakan salah satu strategi hukum yang paling penting untuk melindungi konten di Internet. Perjanjian-perjanjian ini, baik dalam bentuk perjanjian click wrap atau browse wrap, pada umumnya bersifat mengikat, sah, dan dapat dilaksanakan. Agar dapat diterapkan, sangat penting bagi pengguna untuk memiliki kesempatan untuk meninjau persyaratan penggunaan yang berlaku untuk situs. Jika mereka dikubur atau tidak mencolok, mereka akan lebih sulit untuk ditegakkan. Ketentuan penggunaan situs web harus digunakan untuk mengelola, mengalokasikan, mengurangi, membatasi, dan menghindari risiko hukum yang terkait dengan konten dan untuk melindungi hak kekayaan intelektual dan hak properti lainnya di dalam dan untuk konten tersebut. Untuk tujuan artikel ini, konten termasuk konten yang dimiliki oleh situs serta konten pihak ketiga yang dilisensikan atau disediakan untuk situs. Konten juga mencakup konten yang dikirimkan oleh pengguna. Ketentuan kontrak dalam perjanjian syarat penggunaan situs Web harus menangani semua bentuk konten dan risiko hukum yang terkait dengan setiap bentuk konten. Persyaratan kontrak adalah pembelaan hukum tingkat pertama untuk melindungi konten di Internet.

Biasanya, syarat penggunaan situs Web akan menyatakan pada intinya bahwa: "Penggunaan Anda atas situs Web, konten dan layanan yang ditawarkan pada atau melalui situs Web tunduk pada syarat dan ketentuan dalam Persyaratan Penggunaan situs Web ini. Dengan menggunakan Situs Web, Anda setuju untuk terikat oleh dan mematuhi Persyaratan Penggunaan situs Web." Pemilik situs Web biasanya berhak untuk mengubah persyaratan setiap saat untuk memungkinkan layanan baru, masalah baru, dan fleksibilitas di arena

Internet yang dinamis. Penggunaan situs Web secara terus-menerus setelah posting perubahan persyaratan biasanya berarti bahwa pengguna menerima perubahan tersebut.

Akses dan Penggunaan Konten

Persyaratan penggunaan situs web harus memberikan batasan penggunaan konten. Biasanya, istilah "konten" akan didefinisikan secara luas untuk mencakup, namun tidak terbatas pada, semua materi, informasi, teks, grafik, gambar, logo, foto, ilustrasi, klip audio, klip video, dan materi audio visual yang tersedia di Situs web. Definisi konten sering kali akan mencakup contoh spesifik dari jenis konten yang disertakan di situs Web. Perjanjian persyaratan penggunaan situs Web juga digunakan untuk memberikan pemberitahuan bahwa konten dilindungi oleh hak cipta dan undang-undang kekayaan intelektual lainnya dan bahwa pemilik situs Web, afiliasinya, atau pemberi lisensi pihak ketiga memiliki konten tersebut. Sebagian besar perjanjian persyaratan penggunaan melisensikan situs Web yang berlaku untuk menggunakan konten pihak ketiga yang dikirimkan ke situs oleh pengguna secara luas.

Setelah mendefinisikan "konten" dan memberikan pemberitahuan kepemilikan dan perlindungan hak cipta, persyaratan penggunaan situs Web akan memberikan batasan tentang apa yang boleh dilakukan pengguna dengan konten tersebut. Contoh jenis pembatasan dan ketentuan penggunaan yang diizinkan ini adalah sebagai berikut:

Batasan Penggunaan: Anda tidak boleh memodifikasi, menerbitkan, menyalin, mengirimkan, mentransfer, menjual, mereproduksi, membuat karya turunan dari, melisensikan, mendistribusikan, membingkai, hyperlink, mengunduh, memposting ulang, menampilkan, menampilkan, atau dengan cara apa pun mengeksploitasi secara komersial salah satu dari isi; dengan syarat, bagaimanapun, Anda dapat mengunduh satu salinan konten hanya untuk penggunaan pribadi dan non-komersial, asalkan Anda tetap menyimpan semua hak cipta dan pemberitahuan kepemilikan lainnya. Ketentuan ini memberikan lisensi hak cipta terbatas yang mengizinkan pengguna mengunduh konten untuk penggunaan pribadi dan non-komersial pengguna. Jenis lisensi hak cipta terbatas untuk konten ini umum terjadi. Dalam Southwest Airlines Co. v. BoardFirst, L.L.C., pengadilan menemukan bahwa BoardFirst telah melanggar pembatasan Southwest untuk menggunakan situs Web hanya untuk "tujuan pribadi, non-komersial." Pengadilan menyimpulkan bahwa jika BoardFirst mendapat untung dari kesepakatan di mana BoardFirst menggunakan situs Web Southwest untuk mendapatkan boarding pass Kelas A untuk penumpang, maka penggunaannya akan untuk tujuan komersial. Aturan umumnya adalah, jika pengguna melebihi cakupan lisensi hak cipta, pemilik situs Web dapat membawa tindakan hukum terhadap pengguna karena melanggar perjanjian persyaratan penggunaan situs Web dan pelanggaran hak cipta untuk penggunaan konten yang tidak sah, dengan ketentuan bahwa klaim hak cipta di dalam dan pada konten telah didaftarkan ke Kantor Hak Cipta AS. Tujuan dari strategi hukum adalah untuk membuat pemulihan kontrak serta pemulihan pelanggaran hak cipta tersedia jika diperlukan. Semakin besar jumlah upaya hukum yang tersedia, semakin fleksibel perusahaan dalam memerangi pencuri konten.

11.3 KONTEN YANG DIBATASI KATA SANDI

Konten yang Dibatasi Kata Sandi: Beberapa situs Web mungkin berisi area yang dibatasi kata sandi. Area terlarang memungkinkan untuk melindungi konten di area ini dengan

perlindungan hak cipta dan rahasia dagang. Biasanya, perjanjian persyaratan penggunaan situs Web akan menetapkan bahwa, jika pengguna terdaftar sebagai pengguna yang berwenang untuk mendapatkan akses ke area yang dilindungi kata sandi dari situs Web, pengguna akan setuju untuk sepenuhnya bertanggung jawab untuk menjaga kerahasiaan kata sandinya. dan setuju untuk memberi tahu situs Web jika kata sandi hilang, dicuri, diungkapkan kepada pihak ketiga yang tidak berwenang, atau mungkin telah disusupi. Perlindungan kata sandi memberikan lapisan perlindungan lain untuk konten yang mungkin berguna dalam beberapa keadaan. Pembatasan kerahasiaan yang dikenakan pada pengguna dapat menciptakan hubungan kepercayaan dan kepercayaan dengan pengguna sesuai dengan penggunaan perlindungan rahasia dagang. Pengiriman Konten Banyak model bisnis e-niaga dan situs jejaring sosial mendorong pengiriman pengguna atau konten pengguna. Dalam kebanyakan kasus, pengguna mempertahankan kepemilikan konten yang dikirimkannya tetapi memberikan situs Web lisensi yang sangat luas untuk menggunakan konten pengguna. Contoh dari jenis lisensi berikut.

Dengan memposting, mengunggah, memasukkan, menyediakan atau mengirimkan Konten Pengguna Anda ke situs Web, Anda memberikan situs Web, perusahaan afiliasinya, dan sub-lisensi yang diperlukan izin untuk menggunakan Konten Pengguna Anda sehubungan dengan pengoperasian bisnis dan aktivitas situs Web, termasuk, tanpa batasan, hak lisensi untuk menyalin, mendistribusikan, mentransmisikan, menampilkan secara publik, melakukan secara publik, mereproduksi, mengedit, menerjemahkan, dan memformat ulang Konten Pengguna Anda; untuk mempublikasikan nama Anda sehubungan dengan Konten Pengguna; dan hak untuk memberikan hak tersebut kepada pemasok layanan mana pun sehubungan dengan situs Web ini. Ketentuan ini merupakan lisensi hak cipta yang luas dan juga membahas potensi masalah hak publisitas. Ada sejumlah masalah hukum lain yang sering dibahas dalam perjanjian persyaratan penggunaan situs Web sehubungan dengan pengiriman konten pengguna.

Salah satunya adalah bahwa pemilik situs Web akan secara khusus menyatakan bahwa tidak ada kompensasi yang akan dibayarkan sehubungan dengan penggunaan konten pengguna dan bahwa pemilik situs Web tidak berkewajiban untuk memposting atau menggunakan konten apa pun yang mungkin disediakan oleh pengguna dan dapat menghapus pengguna mana pun. konten setiap saat atas kebijakannya sendiri. Sangat penting untuk dapat menghapus atau menonaktifkan akses ke konten pengguna yang mungkin melanggar atau melanggar persyaratan penggunaan situs Web. Ketentuan kontrak harus konsisten dengan kewajiban penghapusan berdasarkan Digital Millennium Copyright Act.

Pencakar, Bot, Perayap, dan Laba-laba: Bot terprogram yang mengikis dan mengumpulkan konten dari situs lain terkadang menargetkan konten. Perusahaan dengan kehadiran online perlu mempertimbangkan kebijakan bot dan skema perlindungannya sebagai bagian dari skema perlindungan konten secara keseluruhan, termasuk penggunaan protokol robots.txt untuk melarang semua bot atau bot tertentu. Perusahaan juga harus mempertimbangkan untuk menggunakan larangan kontrak yang sesuai dengan kebijakan bot untuk mencegah penambangan data, pengikisan, robot, dan metode pengumpulan konten atau ekstraksi konten serupa, seperti berikut:

Penggunaan robot, spider, pencarian situs, aplikasi pengambilan atau perangkat manual atau otomatis lainnya untuk mengambil, mengindeks, mengikis, menambang data atau dengan cara apa pun mengumpulkan atau mengekstrak konten pada atau tersedia melalui Situs atau mereproduksi atau menghindari struktur atau presentasi navigasi dari situs tanpa persetujuan tertulis dari pemilik situs Web adalah dilarang. Perhatikan bahwa persetujuan tertulis yang tegas dapat ditetapkan dalam bot yang diizinkan sehubungan dengan deklarasi robots.txt. Penting untuk menghindari konflik antara ketentuan kontrak dan kebijakan Anda.

Representasi Menghormati Konten Pengguna: Ketentuan kontrak lain yang terkait dengan konten pengguna adalah agar pengguna memberikan jaminan dan representasi terkait konten yang dikirimkan. Contoh dari jenis ketentuan berikut. Dengan memposting, mengunggah, memasukkan, menyediakan, atau mengirimkan Konten Pengguna, Anda menjamin atau menyatakan bahwa Anda memiliki atau mengendalikan semua hak atas Konten Pengguna Anda seperti yang dijelaskan dalam Persyaratan Penggunaan situs Web ini termasuk, tanpa batasan, semua hak yang diperlukan untuk Anda untuk menyediakan, memposting, mengunggah, memasukkan, atau mengirimkan kiriman Konten Pengguna Anda.

11.4 TAMPILKAN PEMBERITAHUAN HAK CIPTA UNTUK MEMBANTU MENCEGAH PENCURIAN KONTEN

Pencuri yang berniat menyalin materi Anda tidak akan digagalkan oleh hal ini, tetapi saya percaya bahwa hal itu akan mengurangi pencurian sampai tingkat tertentu. Ini juga akan membantu melindungi Anda di masa depan jika Anda perlu melawan pencurian, dengan membuktikan bahwa Anda memiliki tanggal hak cipta tertentu yang terkait dengan materi Anda. Jika Anda meneliti hukum hak cipta, Anda tidak perlu secara HARAP mengajukan hak cipta, tetapi hanya bahwa Anda telah menampilkan pemberitahuan hak cipta. Ini karena pengajuan hak cipta yang sebenarnya dapat berlaku surut ke tanggal sebelumnya.

Berikut adalah format pemberitahuan hak cipta tradisional:

HAK CIPTA—– SIMBOL HAK CIPTA—— TANGGAL—— PEMILIK HAK CIPTA

sehingga akan terlihat seperti ini:

Hak Cipta © 1989 Nama Saya

Format di atas berfungsi untuk undang-undang hak cipta AS. Namun, di negara lain dan juga untuk penduduk AS yang ingin melindungi kekayaan intelektual mereka di negara lain

negara, Anda disarankan untuk menambahkan "Semua Hak Dilindungi Undang-Undang." Jadi format yang disukai akan terlihat seperti ini:

Hak Cipta © 1989 Nama Saya Semua Hak Dilindungi Undang-Undang

Tampilkan Peringatan Kuat Bantu Cegah Pencurian Konten

Gunakan teks atau gambar yang menyatakan dengan jelas bahwa menyalin materi Anda dilarang. Berikut adalah beberapa contoh untuk digunakan sebagai titik referensi:

PERINGATAN! DILARANG MENYALIN

PERINGATAN! LARANGAN MENYALIN DIBERLAKUKAN

KAMI AKAN MENUNJUKKAN SEMUA PENCURI INTERNET ATAS MATERI HAK CIPTA KAMI

JANGAN MENYALIN TEKS ATAU GAMBAR KAMI TANPA IZIN KAMI

KAMI MENGHENTIKAN PEMBAJAKAN INTERNET — JANGAN MENYALIN KONTEN KAMI

CUCI KONTEN KAMI, KAMI MENCURI KEBAHAGIAAN ANDA JANGAN SALIN MATERI KAMI DILARANG MENYALIN

JANGAN PERNAH POSTING ULANG MATERI KAMI DI SITUS WEB ATAU BLOG ANDA

Sebenarnya ada lencana dan widget "resmi" yang bisa Anda dapatkan dari beberapa perusahaan seperti CopyScape.com dan kami sendiri, StopWebPirates.com

Nonaktifkan Klik Kanan

Jika Anda memiliki gambar yang tidak ingin disalin orang, atau teks yang tidak ingin disalin orang, ada cara untuk menambahkan sedikit kode ke halaman menggunakan Javascript untuk melakukannya. Tetapi kemudian pengguna yang sah akan frustrasi dan terganggu oleh keputusan Anda untuk melakukan ini. Jadi itu bukan keputusan yang mudah. Juga, pencurian licik selalu dapat "melihat kode sumber" dan MASIH mendapatkan akses ke teks dan gambar Anda, jadi metode ini jelas tidak mudah dilakukan. Karena itu, itu pasti akan menghalangi banyak penyalinan biasa yang akan terjadi dan ini dapat membantu Anda.

Tambahkan kode berikut DI DALAM tag tubuh untuk menonaktifkan fungsi klik kanan mouse DAN salin keyboard. Solusi di atas berfungsi di sebagian besar browser, tetapi tidak semuanya.

Sematkan Konten di Flash

Flash dapat menampilkan konten Anda dan sangat sulit untuk disalin. Tapi masalahnya adalah mesin pencari tidak melihat flash saat ini dan Anda akan mengambil risiko peringkat mesin pencari yang rendah.

Kurangi Bot Spam Penyalinan Otomatis

Terkadang pelanggar terburuk adalah robot spam otomatis. Sayangnya, SEMUA saran di bagian ini akan sangat mengganggu peringkat mesin pencari Anda. Tetapi perlu dimasukkan untuk situasi di mana ini bukan masalah.

- Tempatkan file .htaccess di setiap direktori yang ingin Anda lindungi. File .htaccess melakukan banyak hal, tetapi dalam kasus ini, ia dapat melarang robot web tertentu dan bahkan melarang pengunjung dengan alamat IP dan negara tertentu! Berikut ini adalah artikel bagus tentang cara melakukannya.
- Gunakan Meta Tag untuk mencegah robot mengindeks halaman Anda. Tempatkan kode berikut ke dalam bagian halaman Anda:
- Sematkan konten dalam bingkai Mesin pencari tidak "melihat" konten dalam bingkai sehingga ini akan mengurangi bot spam, tetapi juga mengurangi SEO Anda.
- Password-Lindungi direktori yang berisi halaman web yang ingin Anda lindungi.
- Jelas, tidak ada yang bisa menyalinnya kecuali Anda mengeluarkan kata sandinya. Tapi, tentu saja, halaman Anda juga tidak akan ditampilkan di mesin pencari, jadi Anda harus benar-benar berpikir apakah ini yang Anda inginkan. Berikut adalah artikel bagus tentang cara melakukan ini.
- Gunakan Enkripsi HTML Cukup lakukan pencarian untuk "enkripsi html" dan temukan salah satu dari banyak generator enkripsi di mana Anda cukup menempelkan kode html Anda dan menerima versi terenkripsi. Tempel ulang kode ini ke situs Anda. Browser akan menampilkannya, tetapi robot spam tidak akan melihatnya. (Sayangnya, mesin pencari juga tidak akan melihatnya!)

Gunakan Tautan Mutlak ke Halaman Internal Situs Anda

Kebanyakan orang yang mencuri konten Anda hanya akan mengambilnya dan mempostingnya di situs mereka tanpa menyesuaikan tautan di dalamnya. Jika Anda memiliki tautan relatif seperti ini:

/articles/my_amazing_ info (Ini adalah "tautan relatif.") maka Anda tidak akan mendapat manfaat dari tautan tersebut kembali ke situs Anda. (Setidaknya jika mereka telah mencuri pekerjaan Anda, akan lebih baik jika mereka menautkan kembali ke Anda!)

Tetapi jika Anda membuat hyperlink Anda seperti ini:

http://www.yourdomain.com/articles/my_amazing_ info (Ini adalah "tautan absolut.")

Maka setidaknya Anda akan mendapatkan beberapa lalu lintas ke situs Anda dan SEO Anda akan MENINGKAT.

Tandai Air Gambar Anda

Di sinilah Anda melihat logo atau teks samar ditempatkan DI ATAS gambar, sehingga jika seseorang mencoba menyalinnya, itu akan MEMPERTAHANKAN nama atau logo Anda, atau apa pun yang Anda gunakan sebagai tanda air Anda. Ada banyak program perangkat lunak yang dapat membantu Anda melakukan ini. AiS Watermark Pictures Protector adalah salah satu program watermarking terbaik, memberi Anda kendali penuh.

Gunakan Perangkat Lunak Perlindungan HTML

Biasanya, pendekatan ini tidak diperlukan jika Anda menerapkan beberapa strategi yang tercantum di atas. Tetapi sangat berguna untuk memiliki pendekatan "toko serba ada" jika itu yang Anda inginkan.

Berikut adalah dua yang berkualitas tinggi:

HTML-Protector

Pelindung HTML dari AntSoft

Cara Mencegah Pencurian Gambar dan Bandwidth

"Hotlinking" adalah ketika orang menampilkan gambar Anda di situs web atau blog mereka dengan menautkan ke gambar sebenarnya di situs web ANDA. Jadi, bahkan jika Anda telah memberikan izin untuk menggunakan gambar tersebut, mereka masih "mencuri" bandwidth Anda dan memperlambat situs Anda sendiri dan menghabiskan uang Anda. David Airey datang dengan solusi yang sangat kreatif untuk menangani masalah ini. Anda dapat melihat pendekatannya di sini.

Cara lain untuk mengatasi masalah ini adalah dengan meng-host gambar dan foto Anda di situs hosting gambar gratis seperti Flikr atau Picasa sehingga jika orang melakukan hotlink ke gambar, itu tidak akan memperlambat server Anda atau menghabiskan bandwidth Anda.

Paksa Pencuri untuk Setidaknya Menautkan Kembali ke Anda Untuk Membantu Meningkatkan Lalu Lintas dan SEO Layanan gratis dari EmbedAnything memaksa siapa pun yang menyalin materi Anda untuk menyertakan kode yang menautkan kembali ke Anda. Sangat keren.

Bagaimana jika Konten Anda Bukan Digital Tapi Salinan Digital Ilegal Didistribusikan Melalui Internet?

Misalnya, bagaimana jika Anda telah menulis sebuah buku yang HANYA dalam bentuk fisik tetapi seseorang membuat versi .pdf dari buku ini dan sekarang Anda melihat ini tidak sah "ebook" digital diberikan secara gratis di ratusan situs berbagi file? Itu bisa sangat

membuat frustrasi. Jadi ini tidak akan menghentikan penjahat yang paling keras, tetapi ada baiknya untuk memasang peringatan berikut untuk sedikit membendung arus:
PERINGATAN!
Buku ini hanya dalam bentuk cetak. SEMUA VERSI DIGITAL TIDAK RESMI. Jika Anda mengunggah atau mengunduh versi ebook dari karya ini, Anda melakukan kejahatan dan menyebabkan kesulitan bagi penulisnya. Untuk salinan tambahan buku ini, silakan lihat situs web kami yang mencantumkan sumber sah untuk dibeli: http://www.yourwebsite.com
Disarankan agar Anda menempatkan peringatan di atas pada halaman judul buku Anda atau di suatu tempat yang mencolok di awal.

11.5 HUKUM PENGGUNAAN WAJAR

Ketentuan penggunaan wajar dari undang-undang hak cipta mengizinkan penggunaan atau distribusi materi berhak cipta secara terbatas tanpa izin penulis. Contoh penggunaan materi berhak cipta secara wajar mencakup kutipan kutipan dalam ulasan, pelaporan berita, penelitian, atau penyalinan sebagian kecil karya oleh guru atau siswa untuk mengilustrasikan pelajaran. Ada area abu-abu sejauh mana BANYAK materi yang disalin dan masih dianggap "penggunaan wajar". Ada empat pedoman yang biasanya dipertimbangkan dalam kasus ini:

1. Tujuan dan karakter penggunaan, termasuk apakah penggunaan tersebut bersifat komersial atau untuk tujuan pendidikan nirlaba. Umumnya, jika digunakan untuk tujuan nirlaba, pendidikan, atau pribadi, itu dianggap sebagai penggunaan wajar. Jika untuk penggunaan komersial, maka tidak.
2. Sifat dari karya berhak cipta. Jika apa yang dikutip adalah faktual, maka kemungkinan besar itu adalah penggunaan wajar.
3. Jumlah dan substansi bagian yang digunakan sehubungan dengan karya berhak cipta secara keseluruhan.
4. Pengaruh penggunaan pada pasar potensial untuk, atau nilai, karya berhak cipta. Jika pemilik hak cipta tidak dapat ditentukan, maka itu adalah dianggap penggunaan wajar, tetapi jika materi tersebut melanggar penjualan pemilik hak cipta, maka tidak demikian.

11.6 BAGAIMANA CARA MEMERIKSA APAKAH KONTEN ANDA DICURI?

Berikut adalah beberapa tip mudah tentang cara memeriksa apakah orang telah menyalin materi digital berhak cipta Anda di situs web mereka. Akhir-akhir ini, orang-orang memasang situs web dan tidak berpikir untuk mencuri konten Anda. Ini bisa menjadi teks literal halaman web Anda yang sedang disalin. Atau, bisa juga FILES di website Anda yang juga disalin dan diberikan secara gratis atau bahkan dijual tanpa sepengetahuan Anda. Anda perlu melindungi kekayaan intelektual Anda dengan menggunakan pemeriksa konten duplikat otomatis atau dengan teknik manual. Hanya dengan sedikit usaha, Anda dapat mengatur berbagai pemeriksa plagiarisme yang akan membantu memberikan ketenangan pikiran.

Pindai Web secara Manual untuk Kecocokan dengan Halaman Anda

Mengapa Anda tidak bisa mengetik teks di google? Karena google memiliki maksimum `32 kata yang boleh Anda periksa dalam satu pencarian. Sering kali ini mungkin cukup tetapi bagaimana jika Anda ingin memeriksa untuk melihat apakah sejumlah besar teks dicuri?

Ada banyak layanan web gratis dan berbayar yang tersedia untuk melacak dan memindai halaman Anda untuk memeriksa apakah ada konten yang dicuri di mana saja di web. Beberapa layanan yang saya sarankan adalah:
http://www.copyscape.com http://www.plagiarismchecker.com/ http://www.plagium.com/ http://plagiarism.net/
Gunakan Gambar Google untuk mencari salinan gambar Anda.
Ingatlah untuk menggunakan kutipan di sekitar materi Anda. Jadi, alih-alih mengetik ini: Kisah hidup saya yang luar biasa di New York City
Ketik ini:
"Kisah hidupku yang menakjubkan di New York City"
Alasannya adalah bahwa dengan sebagian besar mesin pencari dan pemeriksa plagiarisme, Anda ingin memeriksa kata-kata ADJACENT. Jika tidak, Anda akan mendapatkan semua situs yang memiliki THE dan STORY dan OF dan MY dan AMAZING, dll. daripada kata-kata itu bersebelahan.
Sematkan Postingan Anda Dengan Pengidentifikasi yang Dapat Dilacak

- Nama file. Cobalah untuk menggunakan nama file yang kreatif atau tidak biasa, yang terkadang bahkan menyertakan salah eja yang disengaja. Dengan cara ini, Anda dapat mencari file seperti itu dan menemukannya lebih mudah daripada file dengan nama yang lebih umum.
- Buat link trik ke halaman situs Anda. Kebanyakan orang hanya akan menyalin materi Anda apa adanya dan tidak meluangkan waktu untuk memperbarui semuanya. Anda dapat melacak tautan masuk dengan situs pemeriksa tautan atau melalui server Anda sendiri dan dengan demikian menemukan situs yang telah menyalin tautan ini. Tautan tersebut dapat berupa tautan yang HANYA mengarah ke halaman situs Anda untuk tujuan ini, bukan ke beranda Anda, yang akan lebih sulit dibedakan dari situs resmi.

Gunakan Plugin Pelacakan Plagiarisme

Jika Anda memiliki situs web berbasis CMS, seperti WordPress, Anda dapat dengan mudah menambahkan perangkat lunak perlindungan salinan dengan plugin pelacakan plagiarisme. http://wordpress.org/extend/plugins/tags/plagiarism untuk daftar saat ini.

Sidik Jari Digital

Buat Kontrol Atas Bagaimana Orang Dapat Menggunakan Konten Anda. Berikut ini adalah plugin WordPress untuk membantu MENGIZINKAN orang untuk menyalin materi Anda sebagai imbalan untuk menerima kredit yang tepat atau bahkan pembayaran!

Sematkan Artikel

iCopyright(R) Article Tools – Mengidentifikasi situs web yang menggunakan kembali konten Anda tanpa izin dan meminta penghapusan atau mengubahnya menjadi pelanggan.

Gunakan Sistem Peringatan Otomatis

Peringatan notifikasi otomatis biasanya tidak gratis. Tetapi mereka sangat membantu karena mereka melacak posting ilegal dari pekerjaan Anda dan mengirimi Anda pengumuman dengan setiap pelanggaran.
http://www.google.com/alerts
http://www.copygator.com

http://plagiarismanalyzer.org
http://checkforplagiarism.net

Gunakan Statistik Web Anda untuk Mengamati Tautan Masuk

- Gunakan Tautan Absolut untuk Halaman HTML: Tautan absolut adalah URL lengkap, misalnya http://www.domainanda.com/folder/page.htm. Jika Anda menggunakan tautan relatif, sangat mudah bagi plagiator untuk menyalin situs web Anda atau halaman web individual ke domain baru. Tautan absolut akan mengharuskan plagiator bekerja lebih keras untuk menghapus atau mengubah semua tautan absolut Anda. Ingat, plagiator itu malas. Jika plagiator gagal mengubah atau menghapus semua tautan Anda, statistik web Anda dapat memberi tahu Anda tentang konten web curian Anda.

11.7 HAK CIPTA KONTEN WEB

Perlindungan hak cipta adalah bagian yang sangat penting dari program untuk melindungi konten. Undang-undang hak cipta melindungi konten asli. Hak cipta hadir dalam karya asli kepengarangan yang ditetapkan dalam media ekspresi apa pun yang nyata, sekarang dikenal atau kemudian dikembangkan, dari mana mereka dapat dirasakan, direproduksi, atau dikomunikasikan, baik secara langsung atau dengan bantuan mesin atau perangkat. Orisinalitas dan fiksasi dalam bentuk nyata adalah dua kriteria mendasar untuk perlindungan hak cipta. Hak cipta terjadi secara otomatis sejak saat penciptaan dan penetapan dalam bentuk nyata.

Orisinalitas adalah prasyarat yang diamanatkan secara konstitusional untuk perlindungan hak cipta. Agar konten dianggap "asli", konten tersebut tidak dapat disalin secara substansial dari karya lain dan harus menunjukkan sedikit kreativitas. Persyaratan orisinalitas ini relatif mudah dipenuhi. Persyaratan tidak menuntut kebaruan atau keunikan hadir. Tidak ada nilai artistik atau keindahan yang dibutuhkan. Ambang batas kreativitas untuk hak cipta cukup rendah. Sebuah karya asli dalam arti hak cipta jika berutang orisinalitasnya kepada penulis dan tidak disalin dari beberapa karya yang sudah ada sebelumnya. Konten asli kemungkinan akan memenuhi persyaratan orisinalitas untuk perlindungan hak cipta.

Sebuah karya dapat menggabungkan materi yang ada dengan izin dari penulis dan masih asli. Ketika sebuah karya yang ada dimasukkan ke dalam sebuah karya baru, hak cipta atas karya baru tersebut hanya berlaku untuk materi asli yang disumbangkan oleh penulis. Jika konten di situs Web tidak asli, pemilik situs Web mungkin masih memiliki hak cipta dalam kompilasi konten. Untuk kompilasi seperti database, orisinalitas hanya dapat diperluas ke pemilihan, koordinasi, dan pengaturan konten. Jika pemilik situs Web telah menyumbangkan konten asli, hak cipta akan diperluas ke teks, foto, grafik, dan konten ekspresif asli lainnya yang disumbangkan serta pemilihan, koordinasi, dan pengaturan konten. Jika pemilik situs Web tidak memberikan kontribusi konten ekspresif asli, maka pemilik situs Web mungkin perlu mengandalkan hak cipta kompilasi. Misalnya, fakta tidak dapat dilindungi oleh hak cipta. Jika pemilik situs Web hanya memberikan kontribusi konten faktual dan konten pihak ketiga, maka dalam keadaan seperti itu pemilik situs Web mungkin hanya dapat menggunakan kompilasi hak cipta.

11.8 PENDAFTARAN HAK CIPTA KONTEN WEB

Kantor Hak Cipta telah menetapkan prosedur untuk pendaftaran hak cipta atas karya online yang tersedia melalui jaringan komunikasi seperti Internet. Prosedur ini berlaku untuk karya yang diakses melalui Internet seperti situs Web, beranda, dan situs FTP serta file dan dokumen yang dikirimkan dan/atau diunduh melalui Internet. Prosedur-prosedur ini tercantum dalam Surat Edaran Kantor Hak Cipta 66-Pendaftaran Hak Cipta untuk Karya Online. Ada juga kemungkinan bahwa klaim hak cipta situs Web dapat didaftarkan dalam beberapa keadaan sebagai program komputer atau sebagai database otomatis.

Untuk semua karya online selain program komputer dan basis data, pendaftaran hanya akan mencakup konten berhak cipta dari karya yang diterima di Kantor Hak Cipta dan diidentifikasi sebagai subjek klaim hak cipta. Untuk karya yang diterbitkan, pendaftaran harus dibatasi pada konten karya yang dinyatakan akan diterbitkan pada tanggal yang diberikan pada aplikasi. Dengan kata lain, jika Anda mengubah konten setelah pendaftaran, pendaftaran tidak akan mencakup konten baru.

Jika pendaftaran untuk program komputer yang membuat tampilan layar saat situs Web dilihat (seperti program yang ditulis dalam html), pendaftaran akan diperluas ke seluruh konten yang dapat dilindungi hak cipta dari kode program komputer. Pendaftaran, bagaimanapun, tidak akan mencakup konten situs Web apa pun yang dihasilkan oleh program yang tidak ada dalam materi pengenal yang diterima oleh Kantor Hak Cipta dan yang tidak dijelaskan pada aplikasi. Untuk semua program komputer lain yang ditransmisikan atau diakses secara online serta untuk setiap database otomatis online yang terdaftar, pendaftaran meluas ke seluruh konten berhak cipta dari situs Web (atau karya online lainnya) yang dimiliki oleh pemilik situs Web, meskipun seluruh konten tidak diperlukan dalam mengidentifikasi materi yang disimpan.

Salah satu masalah yang harus diatasi dalam program pendaftaran hak cipta untuk konten situs Web adalah frekuensi revisi dan pembaruan konten situs Web. Umumnya, revisi berhak cipta untuk situs Web dan karya online lainnya yang diterbitkan pada hari terpisah masing-masing harus didaftarkan secara individual, dengan aplikasi dan biaya pengarsipan terpisah kecuali karya online memenuhi persyaratan pendaftaran grup untuk database atau buletin otomatis. Jika konten situs Web tidak berubah secara signifikan dari hari ke hari, perusahaan dapat mengadopsi strategi pendaftaran terbatas pada pembaruan besar. Strategi lain jika ada perubahan konten baru yang signifikan adalah mendaftarkan situs Web yang direvisi setiap minggu atau setiap bulan tergantung pada tingkat konten baru. Strategi pendaftaran hak cipta harus mencerminkan analisis biaya/manfaat berdasarkan nilai konten berhak cipta dan risiko yang terkait dengan pelanggarannya.

11.9 PENAFIAN TENTANG KONTEN WEB

Penafian: Penafian khusus dapat digunakan berdasarkan sifat konten. Biasanya, penafian ini termasuk dalam persyaratan penggunaan situs Web. Mereka harus menjadi bagian dari perlindungan kontraktual Anda. Satu risiko konten berkaitan dengan keakuratan konten dan kemungkinan kesalahan. Misalnya, penyedia konten sering kali menyatakan bahwa mereka tidak menjamin keakuratan, kegunaan, keandalan, ketepatan waktu, legalitas, atau kelengkapan konten apa pun yang disediakan di atau melalui situs, dan tidak menjamin

bahwa situs akan beroperasi tanpa kesalahan, atau bahwa cacat, kesalahan, atau kelalaian akan diperbaiki, atau bahwa situs tersebut benar-benar aman.

Demikian pula, satu penafian yang umum digunakan sehubungan dengan risiko hukum yang berkaitan dengan menampilkan konten menyatakan bahwa penggunaan konten oleh pengunjung situs di situs Web adalah risiko pengunjung sendiri dan konten yang disediakan di situs Web disediakan "SEBAGAIMANA ADANYA" dan "SEBAGAIMANA TERSEDIA" tanpa jaminan apa pun atas ketersediaan situs dan keakuratan konten yang disediakan. Penafian ini berusaha untuk menjaga dari ketergantungan yang merugikan pada konten yang disediakan. Secara khusus, penafian berusaha meminimalkan ketergantungan yang merugikan dengan memperingatkan pengguna untuk tidak bergantung secara membabi buta pada konten. Penafian mungkin terbukti efektif untuk menjaga terhadap perjanjian yang dibuat dengan implikasi karena penafian secara tegas bertentangan dengan implikasinya. Anda harus menggunakan penafian untuk meniadakan kemungkinan implikasi secara tegas.

Penggunaan penafian lainnya adalah untuk melepaskan tanggung jawab atas konten pihak ketiga yang dapat diakses dari situs Web melalui tautan ke situs Web lain. Sehubungan dengan tautan, biasanya juga bijaksana untuk menyatakan bahwa situs Web tidak bermaksud agar tautan di situs tersebut menjadi rujukan atau dukungan dari entitas terkait atau produk atau layanan apa pun yang disediakan oleh entitas terkait. Penafian adalah bagian dari strategi keseluruhan untuk mengelola risiko yang terkait dengan konten. Menempatkan penafian hanya di beranda situs multi-halaman mungkin tidak cukup, namun, karena pengunjung dapat mengakses berbagai bagian situs Web secara langsung dan bagian berbeda dari situs Web mungkin memerlukan penafian yang berbeda berdasarkan sifat konten, yurisdiksi yang bagian dari situs diarahkan, dan pertimbangan lainnya. Juga bijaksana dalam merancang situs Web untuk menyediakan tautan yang menonjol ke situs Web penafian dan ketentuan penggunaan di bagian bawah setiap halaman Web untuk menekankan penerapannya pada semua konten yang terletak di mana saja atau dapat diakses melalui situs Web dan menjaga kemungkinan - menghubungkan. Pada saat yang sama, praktik ini memastikan bahwa setiap halaman dari situs yang dicetak oleh pengunjung menyertakan referensi ke penafian dan persyaratan penggunaan.

Legenda Hak Milik: Aspek lain dari melindungi konten di Internet adalah penggunaan merek dagang, hak cipta, dan legenda kekayaan intelektual lainnya. Pemberitahuan hak kepemilikan atau legenda di beranda tidak boleh disertakan pada halaman interior tertentu kecuali dirujuk pada setiap halaman yang berlaku. Salah satu pendekatan adalah dengan mempertimbangkan untuk menyertakan logo perusahaan pada setiap halaman situs Web sehingga tidak ada kebingungan dengan siapa pelanggan berurusan serta pemberitahuan kepemilikan dan legenda yang berlaku. Selain pemberitahuan hak cipta Anda, Anda mungkin ingin secara tegas menyatakan: "Tidak ada bagian dari konten ini yang termasuk di situs ini yang boleh direproduksi, diterbitkan ulang, atau didistribusikan kembali tanpa persetujuan tertulis sebelumnya dari Pemilik situs Web" dan perhatikan bahwa penggunaan situs ini diatur oleh perjanjian persyaratan penggunaan situs Web.

Perusahaan harus memanfaatkan alat yang tersedia saat ini untuk menandai konten milik mereka dengan sidik jari elektronik dan memantau dunia maya dengan agen perangkat lunak dan bot untuk menentukan apakah hak kekayaan intelektual mereka di dalam dan atas

konten mereka dilanggar atau disalahgunakan. Salah satu rekomendasinya adalah merancang merek dagang dan logo yang digunakan secara online dengan tujuan memasukkan sidik jari elektronik untuk tujuan menemukannya di dunia maya. Dalam beberapa kasus, mungkin penting untuk tidak hanya menetapkan bahwa konten digunakan tanpa izin, tetapi juga melacak bagaimana penggunaan yang tidak sah itu terjadi.

Beberapa konten dapat diidentifikasi dengan merek dagang atau merek layanan. Penggunaan merek dagang di Internet harus sesuai dengan aturan penggunaan merek dagang umum. Merek dagang yang digunakan di situs Web harus ditandai dengan simbol ™ atau ® yang sesuai, dengan pemberitahuan dari pemilik merek dagang. Ada kecenderungan di Internet untuk tidak mengacaukan situs Web dengan pemberitahuan hukum. Hal ini dapat berakibat fatal bagi pemulihan kerusakan pelanggaran merek dagang. Penting untuk memberi tahu bahwa merek dagang apa pun yang terkait dengan konten telah didaftarkan.

Ketentuan Kontrak Lainnya

Penting juga untuk memastikan bahwa perjanjian persyaratan penggunaan situs Web mencakup batasan kewajiban dan ketentuan kontrak lain yang digunakan untuk mengelola risiko hukum terkait konten. Ketentuan ini dapat mencakup ketentuan penyelesaian sengketa, termasuk ketentuan pemilihan tempat, ketentuan ganti rugi, ketentuan penggunaan yang dapat diterima, dan syarat dan ketentuan umum lainnya. Ketentuan kontrak lainnya ini mungkin terbukti menjadi bagian penting dari keseluruhan program perusahaan untuk melindungi konten di Internet.

Informasi keamanan

Strategi hukum keseluruhan perusahaan untuk perlindungan konten harus diintegrasikan dengan rencana dan kebijakan keamanan informasinya. Mengelola risiko keamanan dari ancaman terhadap konten adalah bagian yang sangat penting dari program perlindungan konten. Manajemen risiko yang hati-hati dan kehati-hatian diperlukan untuk melindungi kerahasiaan, integritas, dan ketersediaan konten informasi. Perusahaan harus memelihara program keamanan informasi yang berisi pengamanan administratif, teknis, dan fisik yang sesuai dengan ukuran dan kompleksitas perusahaan serta sifat dan ruang lingkup kegiatannya yang berkaitan dengan program perlindungan kontennya.

Keamanan yang memadai berarti bahwa perusahaan memelihara keamanan yang efektif yang sepadan dengan risiko, termasuk besarnya kerugian yang diakibatkan oleh akses, penggunaan, pengungkapan yang tidak sah, gangguan, penurunan nilai, modifikasi, atau perusakan informasi. Perusahaan harus menunjuk seorang karyawan atau karyawan untuk mengkoordinasikan dan bertanggung jawab atas program keamanan informasi yang terintegrasi dengan dan melengkapi program perlindungan kontennya. Ini harus mengidentifikasi risiko internal dan eksternal material yang dapat mengakibatkan pengungkapan, penyalahgunaan, perusakan, atau kompromi yang tidak sah terhadap kontennya dan menilai kecukupan perlindungan apa pun yang ada untuk mengendalikan risiko ini.

Sebagai bagian dari program keamanan, perusahaan harus merancang dan menerapkan pengamanan yang wajar untuk mengendalikan risiko yang diidentifikasi melalui penilaian risiko dan secara teratur menguji atau memantau efektivitas pengendalian, sistem, dan prosedur utama pengamanan. Perusahaan juga harus mengevaluasi dan menyesuaikan

program keamanan informasi kontennya berdasarkan hasil pengujian dan pemantauan setiap perubahan material pada program perlindungan kontennya, atau keadaan lain yang diketahui atau memiliki alasan untuk diketahui akan berdampak material pada program keamanan informasinya.

11.10 SOLUSI UNTUK MELINDUNGI KONTEN WEB

Berikut adalah empat hal cepat (dan gratis) yang dapat Anda lakukan untuk melindungi properti Anda dari pencuri online:

1. Sertakan simbol hak cipta di semua halaman situs web Anda dan konten Anda seperti e-book dan donload PDF. Ini akan mencegah mereka yang dengan polosnya berpikir tidak apa-apa menyalin barang-barang Anda tanpa menyadari bahwa itu merupakan pelanggaran.
2. Gunakan Copyscape pemeriksa konten duplikat untuk mencari salinan halaman web atau blog Anda di internet. Anda memasukkan alamat halaman Anda di kotak pencarian dan itu akan memindai web untuk mencari salinannya. Perhatikan bahwa ia mencari setiap halaman satu per satu bukan seluruh situs web.
3. Jika Anda memiliki situs WordPress, coba plug in yang disebut WP-Copyprotect. Ini 'mengunci' blog Anda sehingga teks dan gambar tidak dapat disorot, disalin, dan ditempel. Ini bekerja dengan asumsi bahwa siapa pun yang ingin mencuri posting blog atau teks Anda dari situs web Anda akan terlalu malas untuk mengetik ulang sendiri.

   Saya pikir ini adalah pencegah yang cukup bagus meskipun saya tidak menggunakannya sendiri karena saya selalu menyalin teks dari situs web saya untuk digunakan di tempat lain dan plug in ini akan menghentikan saya melakukan itu!

   Ini mungkin solusi yang baik untuk Anda jika Anda menginginkan cara yang bebas repot untuk melindungi properti online Anda.
4. Lindungi produk, foto, dan gambar online Anda menggunakan lisensi Creative Commons. Anda bisa mendapatkan satu pengaturan dalam hitungan detik secara gratis untuk melindungi eBook, gambar, dan materi lainnya untuk keamanan ekstra itu.

Cara Melindungi Konten Web Hak Cipta

I. Tindakan Pencegahan: Ada tindakan tertentu yang dapat diambil untuk mencegah plagiarisme konten Anda dengan menggambarkan bahwa Anda menyadari hak Anda sebagai pembuat konten.
   1. Daftarkan situs web Anda ke DMCA dan tambahkan salah satu lencana mereka ke situs web Anda untuk memberi tahu calon pelanggar hak cipta bahwa Anda melindungi konten Anda
   2. Sertakan pemberitahuan hak cipta di situs web Anda. Ini akan menunjukkan bahwa Anda mengetahui kedudukan hukum Anda sebagai pembuat konten. Untuk pelanggar yang disengaja, ini mungkin cukup untuk menakut-nakuti mereka. Untuk penyalin yang tidak disengaja, itu harus menjadi pengingat bagi mereka bahwa menyalin konten Anda adalah ilegal. Anda juga dapat

memposting lencana JANGAN SALIN dari situs pemeriksaan konten duplikat seperti PlagSpotter untuk memperingatkan calon plagiator agar tidak mencuri dari Anda.

3. Cara membangun bukti bahwa semua konten Anda benar-benar milik Anda adalah dengan mendokumentasikan proses kreatif secara aktif. Simpan draf semua yang Anda posting secara online jika nanti Anda perlu membuktikan bahwa Anda adalah penulis aslinya.

II. Gunakan Alat Deteksi dan Pemantauan Konten Duplikat: Mendeteksi pelanggaran hak cipta dan bekerja secara pre-emptive terhadap pelanggar dapat menghemat banyak waktu dan tenaga, karena undang-undang hak cipta dapat menjadi kusut dan rumit. Jika Anda memiliki situs web atau blog, setiap dan semua konten yang Anda buat dan unggah harus dipantau terhadap pengambil. Internet penuh dengan alat yang dapat digunakan dalam memerangi pelanggaran hak cipta; berikut adalah alat dan langkah khusus yang dapat diambil untuk melindungi konten web Anda:

1. Gunakan Google Penelusuran untuk memindai internet untuk menemukan bagian unik dari teks Anda. Ingatlah untuk menggunakan tanda kutip agar hasilnya paling akurat dengan struktur kata yang tepat! Cara lain untuk melakukan ini dan menghemat waktu adalah dengan mengatur Google Alerts sehingga setiap kali pekerjaan baru yang cocok dengan permintaan pencarian tersebut dipublikasikan secara online, Google akan memberi tahu Anda melalui email Anda.
2. Pantau konten Anda untuk mencari plagiarisme. Ada berbagai alat yang memungkinkan Anda untuk mencari teks tertentu dan memberi tahu Anda jika bagiannya telah digunakan di tempat lain. Plagium dan Plagiarism adalah dua alat tersebut. Jika kalimat yang digunakan dalam sebuah situs tidak menghubungkan Anda dengan benar, dan Anda adalah penulis aslinya, Anda dapat mengambil tindakan yang diperlukan dan menghubungi situs web plagiator dengan instruksi lebih lanjut.
3. Anda juga dapat menambahkan blog Anda ke layanan Copygator, yang memonitor blog Anda secara gratis dan menghubungi Anda ketika menemukan konten duplikat di internet. Ini memberi label pada konten duplikat sebagai 'tepat' atau 'dekat' untuk menunjukkan apakah konten telah disalin secara identik atau hanya berbagi kemiripan atau elemen serupa satu sama lain.
4. Terkadang kita tidak sengaja menjiplak, entah itu baru saja membaca artikel dan menyalin informasi tanpa maksud atau dengan cara lain. Perangkat lunak PlagSpotter menyediakan layanan yang mirip dengan Copygator tetapi juga memungkinkan Anda untuk memindai konten web Anda menggunakan fitur pencarian batch (kemampuan untuk memeriksa sejumlah besar URL atau seluruh situs Anda) untuk melihat apakah Anda telah menjiplak secara tidak sengaja. Program akan menunjukkan di mana duplikat konten dalam posting atau situs web Anda dan memungkinkan Anda untuk melihat "persentase plagiarisme" Anda. Ini adalah cara praktis untuk memastikan bahwa Anda tidak

akan berakhir di tengah sengketa hak cipta atau dikeluarkan dari hasil pencarian Google.

III. Ambil Tindakan Setelah Menemukan Plagiator: Setelah mengetahui bahwa seseorang telah mengambil konten Anda, Anda perlu melakukan langkah-langkah untuk memperbaiki situasi. Berikut adalah beberapa panduan bermanfaat tentang apa yang harus Anda lakukan untuk memperbaikinya sesegera mungkin.

1. Kumpulkan informasi sebanyak mungkin untuk membuktikan bahwa Anda adalah penulis asli konten tersebut. Ambil tangkapan layar jika memungkinkan.
2. Temukan informasi kontak pelanggar hak cipta. Jika Anda tidak dapat menemukan informasi mereka, coba hubungi webmaster@(apa pun nama domainnya). Anda harus mengirim email sopan yang menyatakan bahwa konten di situs web mereka adalah milik Anda dan digunakan tanpa izin Anda. Minta mereka untuk berhenti dan berhenti dan sertakan semua informasi yang dikumpulkan untuk menunjukkan bahwa Anda memiliki bukti. Dalam kebanyakan kasus, plagiator akan menghapus konten yang dicuri setelah email pertama.
3. Layanan Whosis dapat digunakan untuk menemukan nama resmi dan nomor telepon pemilik situs web. Yang harus Anda lakukan adalah memasukkan nama domain di kotak pencarian dan nama mereka akan muncul. Dari sini, Anda dapat menghubungi mereka dengan ramah dan meminta konten tersebut dihapus.
4. Jika dialog Anda dengan pelaku belum membuahkan hasil, Anda dapat menghubungi perusahaan hosting situs web mereka. Mereka juga dapat ditemukan menggunakan layanan Whois. Beri tahu mereka tentang situasinya dan bahwa orang tersebut menggunakan materi Anda tanpa izin. Mereka dapat menghapus pelanggan.
5. Jika Anda masih belum mendapatkan hasil apa pun, kirimkan surat resmi "Cease and Desist" kepada pelanggar hak cipta. Dengan ini, Anda dapat memberi tahu mereka secara resmi bahwa mereka harus menghapus konten Anda dari halaman web mereka atau menghadapi tindakan hukum yang akan datang. Ada banyak contoh surat "Cease and Desist" online untuk membantu Anda menyusun surat yang meneriakkan "otoritas."
6. Bagian 512 DMCA menyediakan prosedur "pemberitahuan dan penghapusan" yang memberikan cara mudah kepada pemegang hak cipta untuk memutus akses ke konten yang melanggar hak cipta mereka.
7. Ajukan keluhan hak cipta ke Google. Mereka dapat menghapus atau menonaktifkan konten yang melanggar atau menghentikan pelanggan. Formulir untuk melaporkan aktivitas tersebut dan informasi lebih lanjut tentang kebijakan Google dan hubungannya dengan Digital Millennium Copyright Act dapat ditemukan di sini.
8. Pada akhirnya, menggugat plagiator selalu menjadi pilihan; namun, ini termasuk waktu dan pengeluaran, belum lagi stres. Akan direkomendasikan untuk menghabiskan semua jalan lain sebelum mencoba gugatan.

11.11 RINGKASAN

Melindungi konten di Internet memerlukan strategi hukum yang komprehensif tergantung pada sifat konten. Strategi ini mencakup perlindungan kontrak, perlindungan hak cipta (dan mungkin perlindungan kekayaan intelektual lainnya), perlindungan pelabuhan aman Digital Millennium Copyright Act dan perlindungan anti-pengecatan, perlindungan kekebalan dan penggunaan penafian, pemberitahuan, dan legenda kepemilikan. Perlindungan konten perlu memanfaatkan sepenuhnya hak yang diberikan berdasarkan strategi hukum ini. Perlindungan kontrak harus konsisten dengan bentuk perlindungan lain yang diadopsi oleh perusahaan. Dalam unit ini konsep penting dari kontrak situs web, konten yang dibatasi kata sandi, menampilkan pemberitahuan hak cipta untuk membantu mencegah pencurian konten, hukum penggunaan yang adil, cara memeriksa apakah konten Anda dicuri, hak cipta konten web, pendaftaran hak cipta konten web, penafian terkait web konten dan solusi untuk melindungi konten web dibahas panjang lebar untuk pemahaman yang lebih baik tentang hal ini.

11.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Authorpress)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)

- Semua Situs Web yang Relevan dikutip di tempat yang tepat dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

11.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Melindungi situs web Anda dari pencurian sekarang dianggap wajib bagi pemilik situs web.
b) Ketentuan penggunaan situs web harus memberikan batasan penggunaan konten.
c) Beberapa situs web mungkin berisi area yang dibatasi kata sandi.
d) Sifat dari karya berhak cipta, jika apa yang dikutip adalah faktual, maka kemungkinan besar itu adalah penggunaan wajar.
e) Buat tautan trik ke halaman situs Anda.

B. Isi Bagian yang Kosong:

I. Situs web..... merupakan salah satu strategi hukum terpenting untuk melindungi konten di internet.
II. http://www.copyscape.com adalah situs web untuk memeriksa.....
III. Sebuah ..... harus mencerminkan analisis biaya/manfaat berdasarkan nilai konten berhak cipta dan risiko yang terkait dengan pelanggaran.
IV. .....dapat digunakan berdasarkan sifat konten.
V. Sertakan ..... di semua halaman situs web Anda dan baris konten e-book dan unduhan PDF.

11.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Persyaratan penggunaan atau persyaratan perjanjian layanan
2. Plagiarisme
3. Strategi pendaftaran hak cipta
4. Penafian khusus
5. Simbol hak cipta

11.15 PERTANYAAN TERMINAL

1. Apa itu kontrak situs web?
2. Tentukan kata sandi.
3. Apa itu hukum penggunaan wajar?
4. Bagaimana cara memeriksa apakah konten Anda dicuri?
5. Apa solusi untuk melindungi konten web Anda?

BAB 12
PERJANJIAN INTERNASIONAL TENTANG KEAMANAN CYBER

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan International Treatise on Cyber Security
- Memahami sifat dan ruang lingkup Keamanan Siber di berbagai negara
- Memahami masalah teknis dan hukum terkait Keamanan Cyber

12.1 PENGANTAR

Virus komputer Flame adalah program malware digital terbaru yang ditemukan dalam praktik peningkatan serangan dunia maya skala besar. Dua puluh kali lebih besar dari pendahulunya Stuxnet, virus Flame menginfeksi sistem komputer di seluruh Timur Tengah. Analis percaya virus Flame dirancang untuk tujuan spionase, beberapa berpendapat bahwa virus itu tidak memenuhi syarat sebagai "perang dunia maya" (meskipun Kapersky Lab, perusahaan keamanan siber Rusia yang menemukan virus, mengatakan demikian). Namun, motif Stuxnet 2010 tidak diragukan lagi berbahaya. Virus itu menginfeksi fasilitas pengayaan nuklir Iran—yang Iran tegaskan untuk tujuan damai, tetapi banyak yang percaya digunakan untuk mengembangkan senjata nuklir—dan menggagalkan operasi ribuan sentrifugal di beberapa pabrik Iran. The New York Times baru-baru ini melaporkan bahwa Amerika Serikat, dengan bantuan Israel, berada di belakang Stuxnet dalam misi dengan kode nama "Olympic Games."

Sumber pemerintah yang dikutip dalam artikel tersebut menolak untuk mengakui bertanggung jawab atas virus Flame, namun Kaspersky Lab telah menghubungkan Flame dengan Stuxnet. Ambiguitas perang dunia maya mengkhawatirkan para ahli hukum internasional, diplomat, dan komandan militer. Apa yang memenuhi syarat sebagai tindakan perang versus spionase? Apakah hukum "proporsionalitas"—bahwa kerusakan tambahan pada warga sipil dalam pertempuran tidak boleh tidak proporsional dengan target militer yang diserang—berlaku untuk perang dunia maya, terutama karena garis antara sistem komputer sipil dan militer tidak begitu jelas? Haruskah serangan dunia maya oleh peretas tunggal diperlakukan secara berbeda dari yang direkayasa oleh pemerintah nasional? Oleh karena itu, beberapa pakar hukum dan keamanan dunia maya telah menyarankan bahwa sebuah perjanjian internasional, seperti yang dibuat untuk membahas persyaratan perang konvensional, harus dirancang untuk memperjelas aturan perang dunia maya, beberapa bahkan mengusulkan larangan habis-habisan terhadap praktik tersebut. Yang lain bersikeras bahwa perjanjian semacam itu akan sulit bahkan untuk dirancang, dan tidak mungkin untuk ditegakkan.

12.2 KEBIJAKAN KEAMANAN CYBER AS

"Kemakmuran ekonomi Amerika, keamanan nasional, dan kebebasan individu kita bergantung pada komitmen kita untuk mengamankan dunia maya dan mempertahankan

Internet yang terbuka, dapat dioperasikan, aman, dan andal. Infrastruktur penting kita terus menghadapi risiko dari ancaman di dunia maya, dan ekonomi kita dirugikan. oleh pencurian kekayaan intelektual kita. Meskipun ancamannya serius dan terus berkembang, saya percaya bahwa jika kita mengatasinya secara efektif, kita dapat memastikan bahwa Internet tetap menjadi mesin pertumbuhan ekonomi dan platform untuk kebebasan pertukaran ide." (Presiden Obama)

Lima Hal yang Perlu Diketahui: Prioritas Administrasi Keamanan Cyber:

1. Melindungi infrastruktur penting negara — sistem informasi terpenting kami — dari ancaman dunia maya.
2. Meningkatkan kemampuan kami untuk mengidentifikasi dan melaporkan insiden siber sehingga kami dapat merespons secara tepat waktu.
3. Terlibat dengan mitra internasional untuk mempromosikan kebebasan internet dan membangun dukungan untuk dunia maya yang terbuka, dapat dioperasikan, aman, dan andal.
4. Mengamankan jaringan federal dengan menetapkan target keamanan yang jelas dan meminta pertanggungjawaban badan-badan untuk memenuhi target tersebut.
5. Membentuk tenaga kerja yang paham dunia maya dan bergerak melampaui kata sandi dalam kemitraan dengan sektor swasta.

Dunia maya menyentuh hampir setiap bagian dari kehidupan kita sehari-hari. Ini adalah jaringan broadband di bawah kita dan sinyal nirkabel di sekitar kita, jaringan lokal di sekolah dan rumah sakit dan bisnis kita, dan jaringan besar yang menggerakkan bangsa kita. Ini adalah jaringan militer dan intelijen rahasia yang membuat kita tetap aman, dan World Wide Web yang telah membuat kita lebih saling berhubungan daripada kapan pun dalam sejarah manusia. Kita harus mengamankan dunia maya untuk memastikan bahwa kita dapat terus menumbuhkan ekonomi bangsa dan melindungi cara hidup kita.

Administrasi menggunakan prinsip-prinsip berikut dalam pendekatannya untuk memperkuat keamanan siber:

- Pendekatan seluruh pemerintah
- Pertahanan jaringan terlebih dahulu
- Perlindungan privasi dan kebebasan sipil
- Kolaborasi publik-swasta
- Kerjasama dan keterlibatan internasional
- Lindungi Infrastruktur Penting:

Pemerintah harus bekerja sama dengan pemilik dan operator infrastruktur penting untuk melindungi infrastruktur paling sensitif di negara kita dari ancaman keamanan siber. Secara khusus, kami bekerja sama dengan industri untuk meningkatkan pembagian informasi ancaman yang dapat ditindaklanjuti dan peringatan antara sektor swasta dan Pemerintah A.S. dan untuk menyebarkan standar keamanan siber yang dipimpin industri dan praktik terbaik ke perusahaan dan aset infrastruktur penting yang paling rentan.

- Administrasi mengeluarkan E.O. 13636, Meningkatkan Keamanan Cyber Infrastruktur Kritis, pada tahun 2013

- Pemerintah meluncurkan Kerangka Kerja Keamanan Siber lanjutan, sebuah panduan yang dikembangkan secara kolaboratif dengan sektor swasta untuk industri swasta guna meningkatkan keamanan siber mereka, pada tahun 2014

Lindungi Infrastruktur Kritis

Pemerintah harus bekerja sama dengan pemilik dan operator infrastruktur penting untuk melindungi infrastruktur paling sensitif di negara kita dari ancaman keamanan siber. Secara khusus, kami bekerja sama dengan industri untuk meningkatkan pembagian informasi dan peringatan ancaman yang dapat ditindaklanjuti antara sektor swasta dan Pemerintah A.S. dan untuk menyebarkan standar dan praktik terbaik keamanan siber yang dipimpin industri kepada perusahaan dan aset infrastruktur penting yang paling rentan.

- Administrasi mengeluarkan E.O. 13636, Meningkatkan Keamanan Cyber Infrastruktur Kritis, pada tahun 2013
- Pemerintah meluncurkan Kerangka Kerja Keamanan Siber lanjutan, sebuah panduan yang dikembangkan secara kolaboratif dengan sektor swasta untuk industri swasta guna meningkatkan keamanan siber mereka, pada tahun 2014

Tingkatkan Pelaporan dan Tanggapan Insiden

Kita harus meningkatkan kemampuan kita untuk mendeteksi dan mengkarakterisasi insiden dunia maya, berbagi informasi tentangnya, dan merespons secara tepat waktu. Upaya ini mencakup inisiatif pertahanan jaringan, penegakan hukum, dan pengumpulan intelijen, sehingga kita dapat lebih memahami musuh potensial kita di dunia maya.

- Kesadaran akan ancaman atau insiden dunia maya – dan bertindak cepat berdasarkan informasi tersebut – merupakan prasyarat penting untuk respons insiden yang efektif. Seperti yang diarahkan dalam E.O. 13636, Pemerintah A.S. telah mengembangkan sistem dan prosedur untuk meningkatkan ketepatan waktu dan kualitas informasi ancaman dunia maya yang dibagikan dengan entitas sektor swasta yang berisiko. Kami menempatkan penekanan besar pada kesatuan upaya oleh lembaga dengan misi respon domestik.

Terlibat secara Internasional

Karena dunia maya melintasi setiap batas internasional, kita harus terlibat dengan mitra internasional kita. Kami akan bekerja untuk menciptakan insentif untuk, dan membangun konsensus seputar, lingkungan internasional di mana negara-negara mengakui nilai dari ruang siber yang terbuka, dapat dioperasikan, aman, dan dapat diandalkan. Kami akan menentang upaya untuk membatasi kebebasan internet, menghilangkan pendekatan multi-stakeholder terhadap tata kelola internet, atau memaksakan lapisan politik dan birokrasi yang tidak mampu mengikuti kecepatan perubahan teknologi. Ruang siber yang terbuka, transparan, aman, dan stabil sangat penting bagi keberhasilan ekonomi global.

- Kami terus mengejar tujuan kebijakan yang ditetapkan dalam Strategi Internasional A.S. untuk Dunia Maya termasuk:
- Mengembangkan norma perilaku internasional di dunia maya
- Mempromosikan kolaborasi dalam investigasi kejahatan dunia maya (modernisasi Mutual Legal Assistance Treaty)
- Pembangunan kapasitas keamanan siber internasional

Jaringan Federal Aman

Kita harus meningkatkan keamanan semua jaringan federal dengan menetapkan target yang jelas untuk lembaga dan kemudian meminta pertanggungjawaban mereka untuk mencapai target tersebut. Kami juga menerapkan teknologi yang ditingkatkan untuk memungkinkan penemuan dan respons yang lebih cepat terhadap ancaman terhadap data, sistem, dan jaringan federal.

- Sasaran Keamanan Siber Cross Agency Priority (CAP) mewakili prioritas keamanan siber tertinggi Administrasi untuk mengamankan jaringan federal yang tidak terklasifikasi.

Bentuk Lingkungan Cyber Masa Depan

Kami juga melihat ke masa depan. Kami bekerja untuk mengembangkan tenaga kerja yang paham dunia maya dan pada akhirnya membuat ruang maya secara inheren lebih aman. Kami akan memprioritaskan penelitian, pengembangan, dan transisi teknologi dan memanfaatkan inovasi sektor swasta sambil memastikan aktivitas kami terus menghormati privasi, kebebasan sipil, dan hak semua orang.

- Pemerintah federal bermitra dengan sektor swasta dan akademisi untuk mendorong dan mendukung inovasi yang diperlukan untuk membuat dunia maya secara inheren lebih aman.
- Kebijakan dan Inisiatif Keamanan Cyber AS:
- Arahan Kebijakan Presiden 28 (PPD-28) "Sinyal Kegiatan Intelijen", 2014
- Perintah Eksekutif (E.o.) 13636 "Meningkatkan Keamanan Siber Infrastruktur Kritis," 2013
- Arahan Kebijakan Presiden 21 (PPD-21) "Keamanan dan Ketahanan Infrastruktur Kritis," 2013
- Arahan Kebijakan Presiden 8 (PPD-8) "Reformasi Struktural untuk Meningkatkan Keamanan Jaringan Rahasia dan Pembagian dan Pengamanan Informasi Rahasia yang Bertanggung Jawab," 2011
- Tinjauan Kebijakan Dunia Maya, 2009
- Dokumen Pendukung Tinjauan Kebijakan Cyberspace

12.3 ANCAMAN DAN TANTANGAN KEAMANAN CYBER INTERNASIONAL

Dengan meningkatnya proliferasi teknologi informasi dan komunikasi (TIK) dan peluang yang berkembang untuk pertukaran tanpa batas waktu nyata, keamanan dunia maya adalah masalah transnasional yang kompleks yang membutuhkan kerja sama global untuk memastikan Internet yang aman. Menurut sebuah studi Norton 2011, ancaman terhadap dunia maya telah meningkat secara dramatis dalam satu tahun terakhir yang menimpa 431 juta korban dewasa di seluruh dunia - atau 14 korban dewasa setiap detik, satu juta korban kejahatan dunia maya setiap hari. Kejahatan dunia maya kini telah menjadi bisnis yang melebihi satu triliun dolar setahun dalam penipuan online, pencurian identitas, dan kehilangan kekayaan intelektual, yang mempengaruhi jutaan orang di seluruh dunia, serta bisnis yang tak terhitung jumlahnya dan Pemerintah di setiap negara.

Untuk mengatasi masalah dan tantangan seputar keamanan dunia maya dan kejahatan dunia maya, Dewan Ekonomi dan Sosial Perserikatan Bangsa-Bangsa (ECOSOC) mengadakan Acara Khusus tentang "Keamanan dan Pembangunan Cyber", yang

diselenggarakan bersama oleh Departemen Urusan Ekonomi dan Sosial (DESA) dan International Telecommunication Union (ITU) pada 9 Desember di New York. Diketuai oleh Presiden ECOSOC, dengan partisipasi Sekretaris Jenderal ITU dan Ketua Komisi Ilmu Pengetahuan dan Teknologi untuk Pembangunan Perserikatan Bangsa-Bangsa, acara khusus ini mempertemukan Negara-negara Anggota, sistem Perserikatan Bangsa-Bangsa, publik dan swasta sektor, serta organisasi masyarakat sipil lainnya yang tertarik pada bidang keamanan siber dan kejahatan siber.

Pleno dan diskusi panel bertujuan untuk

1) membangun kesadaran di tingkat kebijakan internasional dengan memberikan gambaran kepada Anggota ECOSOC tentang situasi dan tantangan terkini terkait keamanan siber dan kaitannya dengan pembangunan;
2) mengidentifikasi berbagai kebijakan dan inisiatif praktik terbaik yang ada di seluruh dunia untuk membangun budaya keamanan siber; dan (3) jelajahi opsi-opsi untuk respons global terhadap meningkatnya kejahatan dunia maya. Setiap perwakilan di panel membahas berbagai isu seputar keamanan siber, dan perlunya negara-negara anggota, sektor swasta, organisasi masyarakat sipil, dan lembaga penegak hukum untuk bekerja sama mengelola risiko peningkatan interkonektivitas kita. Pembicara membahas peran kesenjangan ekonomi antar negara dan fakta bahwa negara berkembang tidak memiliki kapasitas yang cukup untuk memerangi serangan dunia maya dan kejahatan dunia maya, dan ancaman globalnya terhadap perdamaian dunia maya. Kurangnya kemitraan antara negara maju dan berkembang dapat menghasilkan "tempat berlindung yang aman", di mana penjahat dunia maya dapat memanfaatkan celah hukum, dan kurangnya langkah-langkah keamanan yang kuat terkadang ada di negara berkembang untuk melakukan kejahatan dunia maya. Menarik perhatian pada tantangan melindungi anak-anak secara online, Ms. Deborah Taylor Tate, Utusan Khusus ITU dan Laureate for Child Online Protection, berbagi, "Kita harus mempersenjatai anak-anak kita dengan alat, ketika mereka mengambil langkah pertama dan mengklik di dunia maya. ... Peer to peer dan pengajaran adalah yang terbaik dari advokasi," Dia mendorong orang tua, tokoh masyarakat dan pemerintah untuk mengakses pedoman literasi media yang disediakan secara online oleh ITU.

Selama sesi interaktif, panelis dan negara anggota yang menanggapi membahas perlunya konvensi global di masa depan untuk mengembangkan strategi termasuk kemungkinan membangun Konvensi Budapest, sebuah perjanjian internasional yang berupaya menyelaraskan hukum pidana nasional kejahatan komputer seperti pelanggaran hak cipta, penipuan , pornografi anak, kejahatan kebencian dan pelanggaran keamanan jaringan. Dalam sambutan penutupnya, Presiden ECOSOC, H.E. Lazarous Kapambwe menekankan, "Kami telah sepakat bahwa keamanan dunia maya adalah masalah global yang hanya dapat diselesaikan melalui kemitraan global. Ini mempengaruhi semua organisasi kami.... dan Perserikatan Bangsa-Bangsa diposisikan untuk membawa kemampuan strategis dan analitiknya ke mengatasi masalah-masalah ini."

12.4 KERJASAMA INTERNASIONAL DAN KEAMANAN CYBER

Diluncurkan pada tahun 2007 oleh Sekretaris Jenderal ITU, Dr. Hamadoun I. Touré, Agenda Keamanan Siber Global (GCA) ITU adalah kerangka kerja untuk kerjasama

internasional yang bertujuan untuk meningkatkan kepercayaan dan keamanan dalam masyarakat informasi. GCA dirancang untuk kerjasama dan efisiensi, mendorong kolaborasi dengan dan antara semua mitra terkait dan membangun inisiatif yang ada untuk menghindari upaya duplikasi. Sejak diluncurkan, GCA telah menarik dukungan dan pengakuan dari para pemimpin dan pakar keamanan siber di seluruh dunia. DIA. Óscar Arias Sánchez, Mantan Presiden Republik Kosta Rika dan Peraih Nobel Perdamaian, dan H.E. Blaise Compaoré, Presiden Burkina Faso, keduanya adalah Pelindung GCA. GCA telah memupuk inisiatif seperti Perlindungan Online Anak dan kemitraan ITU-IMPACT, bersama dengan dukungan dari pemain global terkemuka dari semua kelompok pemangku kepentingan, saat ini menyebarkan solusi keamanan siber ke negara-negara di seluruh dunia. PJPK dibangun di atas lima pilar strategis yang disebut juga dengan wilayah kerja:

- Tindakan Hukum
- Tindakan Teknis & Prosedural
- Struktur Organisasi
- Peningkatan Kapasitas
- Kerjasama internasional

Untuk pertama kalinya di tingkat PBB, sekelompok pakar pemerintahan berhasil menyepakati serangkaian rekomendasi penting tentang norma, aturan, dan prinsip perilaku yang bertanggung jawab oleh negara-negara di dunia maya. Pakar pemerintahan dari lima anggota tetap Dewan Keamanan PBB dan 10 kekuatan dunia maya terkemuka dari seluruh wilayah di dunia telah mengakui bahwa hukum internasional, termasuk prinsip-prinsip hukum tanggung jawab negara, sepenuhnya berlaku untuk perilaku negara di dunia maya. Pengakuan ini merupakan langkah penting menuju penerimaan universal kerangka hukum. Ketidakjelasan aturan sebelumnya di dunia maya menjadi salah satu faktor penyebab ketidakstabilan dan risiko eskalasi.

Penegasan eksplisit bahwa hukum internasional, khususnya prinsip-prinsip Piagam PBB, dapat diterapkan pada aktivitas negara di dunia maya, termasuk aktivitas aktor non-negara yang terkait dengan negara, akan memungkinkan komunitas internasional dan negara yang terkena dampak untuk bereaksi terhadap pelanggaran secara lebih efektif. Di dunia maya, negara harus mematuhi larangan penggunaan kekuatan, persyaratan untuk menghormati kedaulatan dan kemerdekaan teritorial, dan prinsip penyelesaian perselisihan dengan cara damai dengan cara yang sama seperti di dunia fisik. Hak, yang ditentukan dalam Pasal 51 Piagam PBB, untuk membela diri termasuk penggunaan kekuatan akan berlaku jika serangan dunia maya mencapai tingkat "serangan bersenjata." Namun, laporan tersebut menahan diri untuk tidak menyebutkan kapan hal ini bisa terjadi karena perdebatan hukum tentang masalah ini baru saja dimulai.

Prinsip-prinsip hukum universal ini melampaui pembatasan penggunaan kekuatan di dunia maya. Mereka juga mencakup bidang lain seperti kedaulatan dan integritas teritorial, yang membatasi keabsahan tindakan yang berpotensi membahayakan di bawah tingkat kekuatan kinetik. Secara khusus, bersama dengan prinsip-prinsip hukum kebiasaan internasional tentang tanggung jawab negara, prinsip-prinsip Piagam PBB akan membatasi legitimasi tindakan negara yang dengan sengaja melanggar kekayaan intelektual perusahaan atau data pribadi individu. Namun demikian, para ahli hukum perlu melakukan lebih banyak

pekerjaan untuk menentukan prinsip-prinsip dan aturan-aturan ini untuk mencakup secara lebih spesifik berbagai tindakan yang beragam di dunia maya. Atribusi terus menjadi tantangan utama, karena atribusi hukum dan teknis diperlukan untuk menantang suatu negara, misalnya, di Dewan Keamanan, atas tindakan yang salah di dunia maya.

Mengenai serangan siber yang mencapai ambang batas konflik bersenjata, ambang batas yang lebih rendah dari serangan bersenjata, sebagian besar dari 15 ahli bersedia secara eksplisit mengakui penerapan hukum humaniter internasional ke dunia maya.

Rusia telah menerima penerapan hukum tersebut ke dunia maya. China, di sisi lain, telah berulang kali menyatakan bahwa mereka menganggap konfirmasi eksplisit seperti itu terlalu dini dan bertentangan dengan tujuan mencegah serbuan senjata siber ofensif. Pekerjaan di masa depan oleh Komite Palang Merah Internasional atau oleh organisasi non-pemerintah seperti East West Institute mungkin membuka jalan bagi pengakuan semacam itu oleh China juga. Laporan kelompok ahli mengulangi pernyataan dari laporan kelompok ahli 2010 tentang perlunya pemahaman bersama tentang bagaimana norma tersebut berlaku untuk perilaku negara dan penggunaan TIK oleh negara, serta kemungkinan mengembangkan aturan perilaku yang lebih spesifik.

Membangun Transparansi dan Kepercayaan: Pada isu kontroversial tentang bagaimana menghadapi kemungkinan yang meningkat dari negara-negara tersebut untuk mengejar pengembangan senjata siber, kelompok tersebut berhasil mengambil pendekatan yang realistis. Dalam rancangan kode etik mereka mengenai penggunaan TIK oleh negara-negara, yang diserahkan kepada sekretaris jenderal PBB pada tahun 2011, Cina dan Rusia menyarankan larangan eksplisit dari apa yang mereka sebut "senjata informasi" dan proliferasi teknologi mereka.

Namun, dalam pembahasan kelompok ahli, perwakilan China dan Rusia mengakui sifat ganda yang melekat pada teknologi ini dan bergabung dengan pendekatan yang lebih pragmatis untuk memulai dengan langkah-langkah membangun kepercayaan tradisional dan langkah-langkah kooperatif lainnya sebelum mencoba menyepakati larangan yang pada dasarnya tidak dapat diverifikasi. Pada saat yang sama, para ahli memahami bahwa langkah-langkah membangun kepercayaan dapat menjadi titik awal jika pendekatan pengendalian senjata menjadi layak di masa depan.

Dalam beberapa paragraf, laporan kelompok tahun 2013 mengacu pada bahasa yang digunakan dalam perjanjian lain dengan implikasi pengendalian senjata. Secara khusus, laporan tersebut menyerukan kepada negara-negara bagian untuk mempromosikan lingkungan TIK yang "damai", yang dapat dipahami sebagai acuan terhadap apa yang disebut klausul "tujuan damai" dari Perjanjian Luar Angkasa. Dalam pendekatannya terhadap isu-isu dunia maya, kelompok ahli menerapkan konsep serupa dengan menahan diri untuk tidak memberlakukan larangan tertentu tetapi mengedepankan tujuan umum penggunaan ruang dunia maya oleh negara secara damai. Hal ini memperkuat kemampuan kesepakatan masa depan untuk mencakup perkembangan masa depan di lapangan.

Menyadari bahwa langkah-langkah membangun kepercayaan dan pertukaran informasi antar negara sangat penting untuk meningkatkan prediktabilitas dan mengurangi risiko salah persepsi dan eskalasi melalui ancaman siber, kelompok ahli menyepakati serangkaian tindakan sukarela untuk mempromosikan transparansi dan kepercayaan di antara

negara-negara di bidang ini. Langkah-langkah tersebut bertujuan untuk meningkatkan transparansi dan menciptakan atau memperkuat hubungan komunikasi untuk mengurangi kemungkinan bahwa insiden siber yang disalahpahami dapat menciptakan ketidakstabilan internasional atau krisis yang mengarah pada konflik. Secara bersama-sama, mereka mewakili landasan penting bagi langkah-langkah bilateral, regional, dan global untuk membangun kepercayaan dan stabilitas global di dunia maya dan untuk mencegah eskalasi insiden keamanan dunia maya yang tidak perlu.

Secara khusus, laporan tersebut merekomendasikan langkah-langkah membangun kepercayaan berikut:

- Bertukar pandangan dan informasi tentang kebijakan nasional, praktik terbaik, proses pengambilan keputusan, serta organisasi dan struktur nasional terkait keamanan siber. Sebagai contoh, Amerika Serikat pada tahun 2012 dan Jerman pada tahun 2013 saling bertukar buku putih tentang pertahanan siber dengan Rusia.
- Membuat kerangka konsultatif bilateral atau multilateral untuk langkah-langkah membangun kepercayaan, misalnya, di dalam Liga Arab, Uni Afrika, Forum Regional Perhimpunan Bangsa-Bangsa Asia Tenggara (ASEAN), Organisasi untuk Keamanan dan Kerjasama di Eropa (OSCE) , dan Organisasi Negara-Negara Amerika. Kerangka kerja ini dapat mencakup lokakarya dan latihan tentang cara mencegah dan mengelola insiden keamanan siber yang mengganggu.
- Meningkatkan pembagian informasi dan komunikasi krisis antar negara tentang insiden keamanan siber di tiga tingkat: antara CERT nasional secara bilateral dan dalam komunitas CERT multilateral yang sudah ada untuk bertukar informasi teknis tentang malware atau indikator berbahaya lainnya; melalui saluran yang sudah ada atau yang baru dibuat untuk manajemen krisis dan peringatan dini untuk menerima, mengumpulkan, menganalisis, dan membagikan informasi tersebut untuk membantu mengurangi kerentanan dan risiko; dan melalui saluran dialog di tingkat politik dan kebijakan.
- Meningkatkan kerjasama untuk mengatasi insiden yang mempengaruhi sistem infrastruktur penting, terutama yang bergantung pada sistem kontrol industri berbasis TIK.
- Meningkatkan mekanisme kerjasama penegakan hukum untuk mengurangi insiden yang dapat disalahpahami sebagai tindakan negara yang bermusuhan dan yang mempengaruhi keamanan internasional.

Meskipun pemerintah harus memimpin dalam mengembangkan dan menerapkan langkah-langkah ini, kelompok tersebut mengulangi dan menyoroti peran penting yang harus dimainkan oleh sektor swasta dan masyarakat sipil dalam upaya ini. Dalam pekerjaan di masa depan, pemerintah dan sektor swasta harus melakukan upaya bersama untuk menguraikan tujuan, kondisi, persyaratan, kerangka kerja dan model kemitraan publik-swasta untuk keamanan siber internasional dalam skala global. Beberapa perusahaan ICT global sudah terlibat dalam diskusi ini. Namun, peran khusus negara dan perusahaan swasta serta batasan kerjasama di antara mereka di bidang keamanan siber yang sensitif perlu dikembangkan lebih jelas oleh pemerintah dan pemangku kepentingan sektor swasta.

Dalam laporannya, kelompok ahli menyoroti perlunya pembangunan kapasitas internasional untuk membantu negara-negara dalam upaya mereka mengatasi kesenjangan digital dan untuk meningkatkan keamanan infrastruktur TIK yang vital. Laporan tersebut menyerukan kepada negara-negara bagian, yang bekerja dengan sektor swasta dan badan-badan khusus PBB, untuk memberikan bantuan teknis atau bantuan lainnya dalam membangun kapasitas dalam keamanan TIK. Secara khusus, bantuan tersebut dapat membantu memperkuat kerangka hukum nasional dan kemampuan serta strategi penegakan hukum, memerangi penggunaan TIK untuk tujuan kriminal atau teroris, dan memperkuat kemampuan respons insiden, termasuk melalui kerjasama CERT-ke-CERT.

12.5 KONVENSI UNI AFRIKA TENTANG KEAMANAN CYBER DAN PERLINDUNGAN DATA

Konvensi ini diadopsi selama Sesi Biasa ke-23 dari KTT Uni Afrika yang berakhir di Malabo, Guinea Khatulistiwa pada tanggal 27 Juni 2014. Konvensi, yang untuk pertama kalinya secara substantif membawa bahasa 'perlindungan provokasi pribadi' ke tingkat ini , berusaha membangun kerangka hukum untuk Keamanan Siber dan Perlindungan Data Pribadi khususnya dalam konteks e-niaga. Ini dibangun di atas komitmen yang ada dari Negara-negara Anggota Uni Afrika di tingkat sub-regional, regional dan internasional untuk membangun Masyarakat Informasi. Versi yang diadopsi merupakan perbaikan dari versi sebelumnya, yang banyak dikritik oleh beberapa pemangku kepentingan, termasuk oleh kelompok masyarakat sipil, terutama karena kegagalannya untuk melindungi hak privasi secara memadai.

Konvensi mengakui pentingnya kepatuhan terhadap konstitusi nasional dan hukum internasional, misalnya dalam pembukaannya Konvensi menyatakan bahwa pembentukan kerangka peraturan tentang keamanan siber dan perlindungan data pribadi harus mempertimbangkan persyaratan penghormatan terhadap hak-hak warga negara. , dijamin di bawah teks dasar hukum domestik dan dilindungi oleh Konvensi dan Perjanjian hak asasi manusia internasional, khususnya Piagam Afrika tentang Hak Asasi Manusia dan Rakyat. Persyaratan ini ditekankan lebih dari sekali dalam teks.

Yang penting, Konvensi memerintahkan negara-negara pihak untuk menetapkan kerangka hukum dan kelembagaan untuk perlindungan data dan keamanan siber. Namun dalam kasus keamanan siber, negara dapat mendirikan lembaga baru atau menggunakan lembaga yang sudah ada sebelumnya. Persyaratan ini, jika diterapkan dengan benar, dapat membantu menghadirkan elemen akuntabilitas dalam cara kerja polisi dan dinas keamanan dan diatur di benua itu.

Konvensi juga menguraikan prinsip-prinsip yang harus dipatuhi dalam memproses data pribadi, seperti persetujuan dan legitimasi; keabsahan dan keadilan; tujuan, relevansi, dan penyimpanan data pribadi yang diproses; ketepatan; transparansi serta kerahasiaan dan keamanan data pribadi. Selanjutnya memerintahkan negara pihak untuk melarang pengumpulan dan pemrosesan data apa pun, tanpa persetujuan, yang mengungkapkan asal ras, etnis dan daerah, afiliasi orang tua, pendapat politik, keyakinan agama atau filosofis, keanggotaan serikat pekerja, kehidupan seks dan informasi genetik atau, lebih umum, data tentang keadaan kesehatan subjek data, kecuali dalam keadaan luar biasa tertentu.

Sekilas Kelemahan: Pertama, mengingat kelemahan yang melekat pada sebagian besar mekanisme sektor keamanan Afrika, khususnya, sifat partisan dan kompromi dari sektor

keamanan negara dan pendaftaran data kependudukan, Konvensi dapat memasukkan persyaratan pengawasan yudisial yang kuat agar untuk memperkuat perlindungan hak atas privasi dan menahan pengaruh politik pada pengelolaan data, khususnya data dalam perjalanan, penyimpanan, cloud, atau saat tidak digunakan.

Kedua, meskipun Konvensi tersebut memerintahkan negara-negara pihak untuk memberlakukan undang-undang yang mempertimbangkan konstitusi dan konvensi internasional mereka, Konvensi ini hanya terlalu menekankan Piagam Afrika. Mengingat bahwa Piagam Afrika tidak memiliki hak eksplisit atas privasi sehubungan dengan akses ke informasi dan pemrosesan data pribadi, ini menciptakan celah yang perlu diisi.

Ada juga banyak contoh di mana Konvensi tampaknya menempatkan kedaulatan dan kebijaksanaan nasional atas hukum internasional, misalnya, di bawah Bab 3 tentang Mempromosikan keamanan dunia maya dan memerangi kejahatan dunia maya, Konvensi menggunakan ograses sebagai, 'sebagaimana dianggap perlu, sebagaimana dianggap tepat dan karena dianggap efektif'. Diskresi yang begitu luas, memberikan ruang bagi negara-negara, terutama yang tidak demokratis, untuk menyalahgunakan kekuasaan ini. Hal ini terutama terjadi karena Konvensi tidak secara eksplisit menguraikan ambang batas minimum yang harus dipenuhi dan dipatuhi oleh konstitusi nasional, kerangka hukum dan undang-undang. Dalam hal ini, referensi eksplisit terhadap hukum internasional akan sangat membantu.

Memberikan keleluasaan yang luas kepada negara-negara pihak tentang isi undang-undang dan konstitusi mereka tidak sejalan dengan praktik terbaik dan rekomendasi internasional saat ini tentang masalah tersebut. Terkait dengan hal ini, Komite Hak Asasi Manusia memberikan panduan penting dalam Komentar Umum 16 tentang interpretasi pasal 17 Kovenan Internasional tentang Hak Sipil dan Politik. Menurut Komite, istilah "melawan hukum" berarti bahwa tidak ada campur tangan yang dapat terjadi "kecuali dalam kasus-kasus yang diatur oleh undang-undang. Campur tangan yang diizinkan oleh Negara hanya dapat terjadi atas dasar hukum, yang dengan sendirinya harus memenuhi ketentuan, tujuan dan tujuan Kovenan" [penekanan ditambahkan].

Juga menjadi perhatian, sementara Pasal 15 yang berkaitan dengan interkoneksi file data pribadi merupakan perkembangan positif dari sudut pandang skema perlindungan komersial dan sosial, mengingat bahwa Konvensi tidak menentukan ambang batas minimum yang harus dipenuhi oleh kerangka hukum yang diusulkan, contoh penciptaan big data dan berbagi data tanpa syarat yang ketat dan pengawasan yudisial dasar tentu akan mengarah pada peningkatan pengawasan dan pemantauan negara sehingga menyebabkan erosi privasi dan kebebasan sipil lainnya.

Praktik semacam itu telah banyak dikritik di negara-negara seperti Zimbabwe di mana parlemen baru-baru ini mengeluarkan laporan yang merugikan tentang skema pendaftaran kartu SIM. Skema tersebut melibatkan, antara lain, pembuatan database bersama seperti yang direncanakan di bawah Konvensi. Selain itu, laporan pers baru-baru ini melaporkan tentang bagaimana Zimbabwe diduga mendirikan proyek Komputer Tingkat Tinggi (HCL) yang memerlukan pendirian laboratorium super-informasi yang akan mengumpulkan informasi dari hampir semua departemen pemerintah dan sektor swasta untuk perencanaan, penelitian

dan tujuan pembangunan. Dianggap sebagai yang pertama dari jenisnya di Afrika, juga dilaporkan bagaimana otoritas negara telah menyusup ke fasilitas tersebut.

Kelemahan-kelemahan di atas, sama sekali bukan berarti kurangnya pengakuan bahwa Konvensi Uni Afrika meletakkan landasan progresif, yang mungkin untuk pertama kalinya, mendorong negara-negara untuk menjelaskan bidang vital layanan keamanan yang kebanyakan orang anggap gelap dan dalam. kebutuhan transparansi. Namun, di tingkat kontinental, selain Konvensi, Uni Afrika harus mengambil satu langkah lagi dengan memperkenalkan hak privasi dalam Piagam Afrika. Mereka dapat, misalnya, memperkenalkan Protokol Opsional sejalan dengan rekomendasi yang kami buat dalam makalah kami yang dipresentasikan di Forum LSM Sesi ke-55 Komisi Afrika.

Kedua, sementara sebagian besar negara Afrika telah mengambil langkah terpuji untuk memasukkan hak privasi dalam konstitusi nasional mereka, menurut artikel 'Tata Kelola Internet: Mengapa Afrika harus memimpin dan' Hukum Privasi Data Global: 89 Negara, dan Mempercepat; di Afrika hanya 11 negara yang telah memberlakukan undang-undang kebebasan informasi/berekspresi nasional dan delapan Negara Afrika tentang hak atas privasi/perlindungan data. Oleh karena itu, negara-negara Afrika harus segera mengambil langkah-langkah untuk mengadopsi undang-undang perlindungan data dan memperkuat ketentuan konstitusional yang sejalan dengan Konvensi, terlepas dari kelemahannya yang disebutkan di atas.

12.6 KONVENSI DEWAN EROPA TENTANG KEJAHATAN CYBER (KONVENSI BUDAPEST)

Budapest Convention Cybercrime, atau disebut sebagai Budapest Convention atau Convention Cybercrime adalah perjanjian internasional pertama yang bertujuan untuk mengatasi dan mengatasi kejahatan komputer dan internet dengan menyelaraskan undang-undang negara, meningkatkan teknik penyelidikan selain meningkatkan kerja sama negara-negara dalam hal hukum komputer.

Perjanjian itu dirancang untuk menyelesaikan kejahatan yang dilakukan melalui internet di antara jaringan lain, menangani pelanggaran hak cipta, penipuan terkait komputer, gambar anak-anak yang tidak senonoh, kejahatan kebencian dan pelanggaran terhadap sekuritas jaringan. Konvensi Budapest tentang tujuan utama kejahatan dunia maya meliputi:

- "Mengharmoniskan unsur-unsur hukum substantif pidana domestik dari pelanggaran dan ketentuan terkait di bidang kejahatan dunia maya."
- "Menyediakan kekuatan hukum acara pidana domestik yang diperlukan untuk penyelidikan dan penuntutan pelanggaran tersebut serta pelanggaran lain yang dilakukan melalui sistem komputer atau bukti yang terkait dengan yang berasal dari elektronik."
- "Membentuk rezim kerja sama internasional yang cepat dan efektif."
- Siapa yang telah mendaftar? Per September 2012 ada total:
- 37 pihak termasuk 35 negara Eropa, Amerika Serikat dan Jepang.
- 10 penandatangan yang terdiri dari 8 negara Eropa, Kanada dan Afrika Selatan.
- 8 negara bagian yang ingin bergabung termasuk Argentina, Australia, Chili, Kosta Rika, Republik Dominika, Meksiko, Filipina, dan Senegal.
- 55 negara bagian sedang atau berkomitmen untuk menjadi pihak.

Banyak negara enggan menandatangani perjanjian tersebut dengan dasar bahwa ketika Konvensi Budapest Cybercrime pertama kali dirancang pada tahun 2001, itu disesuaikan dan diarahkan ke negara-negara Eropa dan diyakini agak ketinggalan jaman. Brasil mempertimbangkan untuk menandatangani Budapest Convention Cybercrime tetapi kemudian menolak karena meningkatkan kekhawatiran tentang ketentuan konvensi mengenai kriminalisasi pelanggaran kekayaan intelektual, yang diyakini Brasil bukan ketentuan yang cocok untuk model universal.

Di seluruh dunia ada perbedaan pandangan yang jelas mengenai apa yang akan membuat standar global yang sesuai dan oleh karena itu menyesuaikan Kejahatan Siber Konvensi Budapest agar sesuai dengan kebutuhan semua orang secara global akan menjadi tugas yang hampir mustahil. Dengan ketidaksepakatan mengenai pedoman perjanjian itu: Rusia, Tajikistan dan Uzbekistan mengirim surat ke PBB meminta resolusi untuk kode melakukan di dunia maya, membuat ketentuan yang dimaksudkan untuk menghentikan penggunaan internet oleh teroris.

Banyak negara termasuk Amerika telah melihat proposal dengan kecurigaan percaya bahwa itu mungkin telah dibuat sebagai maksud sebagai instrumen hukum yang dapat digunakan untuk secara tidak adil menindak perbedaan pendapat berbasis Internet. Lagi-lagi membuktikan bahwa menghasilkan konsensus untuk kode etik perjanjian itu adalah tugas yang sangat sulit dan kemungkinan besar tidak mungkin. Sampai saat ini, masa depan Budapest Convention Cybercrime masih belum jelas; undang-undang kejahatan dunia maya diperlukan tetapi spekulasi tentang apakah Budapest harus menjadi undang-undang itu dipertanyakan.

Budapest Convention Cybercrime adalah satu-satunya perjanjian internasional yang diterima yang bekerja untuk melindungi orang dan hak-hak mereka terhadap kejahatan online. Di bawah perjanjian ini, negara-negara dapat mendefinisikan tindakan kriminal terhadap dan menggunakan komputer, menyediakan penegakan hukum dengan alat investigasi dan membuat titik kontak untuk kasus-kasus mendesak internasional hampir setiap hari.

Jumlah pihak yang telah menandatangani Konvensi Budapest Cybercrime dan telah membawa undang-undang negara mereka sesuai dengan kode etik perjanjian telah meningkat - sekitar 140 dari 193 anggota PBB telah mereformasi undang-undang mereka yang berkaitan dengan kejahatan dunia maya, dengan di setidaknya 125 di antaranya menggunakan Budapest Convention Cybercrime sebagai sumber inspirasi. Semua ini telah berkontribusi pada globalisasi hukum pidana yang berkaitan dengan komputer.

Telah dilaporkan bahwa Microsoft telah mengatakan bahwa "Dewan Eropa telah berhasil karena telah membantu mendorong pemerintah untuk memberlakukan undang-undang kejahatan dunia maya di dalam negeri dan bekerja untuk memerangi kejahatan dunia maya internasional. Dewan ini berfokus pada masalah kepentingan lintas yurisdiksi yang melayani kepentingan banyak negara. daripada sedikit." Menunjukkan bahwa perubahan nyata untuk kebaikan telah terjadi karena perjanjian itu.

Terlepas dari kebaikan yang telah dibuat, sejumlah negara termasuk China dan Rusia, menginginkan lebih banyak kontrol atas Internet, menentang Kejahatan Dunia Maya Konvensi Budapest dan sebaliknya ingin menyerukan perjanjian internasional baru. Sampai saat ini,

belum ada konsensus ke arah ini dan mungkin tidak akan terjadi untuk sementara waktu; Butuh lebih dari sepuluh tahun untuk mempersiapkan Konvensi Budapest tentang Kejahatan Dunia Maya, negosiasi perjanjian baru yang bertujuan untuk melampaui Konvensi Budapest akan menjadi tugas yang sulit. Kontroversi terhadap perjanjian tersebut berisiko tidak hanya mengganggu reformasi yang terjadi di banyak negara, tetapi juga merusak semua kegiatan bantuan teknis dan mempertajam perpecahan internasional yang telah dilakukan.

12.7 KEAMANAN PERTAHANAN CYBER: POSISI INDIA

Posisi India saat ini di tingkat internasional dalam keamanan siber sebagian besar berasal dari tradisi multilateralisme yang diwarisi Kementerian Luar Negeri, yang sangat dipengaruhi sejak tahun 1970-an oleh dimensi Utara-Selatan. Pembentukan keamanan nasional di Delhi, bagaimanapun, sadar akan kebutuhan mendesak untuk membangun kemampuan domestik. Kaum realis tidak punya waktu untuk bermegah di panggung global tentang isu-isu dunia maya. Pendekatan India terhadap masalah keamanan internasional di masa lalu didominasi oleh prinsip-prinsip kesetaraan dan non-diskriminasi. Namun, sebagai kekuatan potensial dalam dirinya sendiri, India mungkin harus mengukir jalan yang pasti akan menyimpang dari pendekatan tradisionalnya terhadap keamanan internasional. Seperti dalam domain nuklir, demikian juga di dunia maya, kepentingan nasional India mungkin tidak sejalan dengan posisi kolektif Selatan. Tantangan utama India adalah membawa pragmatisme ke dalam keterlibatannya dalam masalah keamanan dunia maya yang dapat secara efektif menggabungkan prinsip tradisional internasionalisme dengan dinamika strategis yang berkembang di domain dunia maya.

Sebagai negara-negara besar yang paling lemah, India harus belajar dengan gesit menavigasi dinamika di antara negara-negara besar dalam masalah keamanan siber. Di masa lalu, India sering mendesak negara-negara besar untuk mematuhi norma-norma dalam pengelolaan tantangan keamanan, tetapi sangat terganggu oleh kolaborasi apa pun antara negara-negara besar. Misalnya, India sangat prihatin tentang kontrol senjata nuklir bilateral antara Washington dan Moskow dan implikasi dari kejuaraan bersama rezim non-proliferasi. Saat ini, India mengkhawatirkan konsekuensi potensial dari perjanjian keamanan siber yang mungkin muncul dari negosiasi bilateral antara Amerika dan China. India juga harus menyadari fakta bahwa perubahan teknologi dan kebangkitan kekuatan baru menghasilkan tekanan untuk menulis ulang aturan internasional. India memang telah meningkatkan keterlibatannya dengan negara-negara besar dalam masalah keamanan siber.

Keterlibatan ini tertatih-tatih oleh pemerintah yang lemah di Delhi yang tidak mampu mengesampingkan masing-masing departemen dalam membuat kebijakan penting. Dengan pemerintah pusat yang kuat sekarang berada di bawah kepemimpinan Narendra Modi, pertimbangan keamanan nasional dan keseimbangan kekuatan cenderung memiliki arti penting yang lebih besar dalam pendekatan internasional India terhadap masalah dunia maya. Karena domain siber menarik perhatian dari pemerintah Modi, India harus melihat ke arah membangun koalisi fungsional untuk mengamankan kepentingannya sendiri di arena global. Dengan cara apa pun India memandang masalah keamanan siber, AS tampak besar. Meskipun demokrasi, pertimbangan keamanan internal sering menempatkan India bertentangan dengan AS dan di sisi yang sama dengan Rusia dan China dalam beberapa aspek regulasi siber.

Namun pertimbangan yang lebih luas dari rezim internasional yang membangun keamanan siber, dan dorongan baru untuk kemitraan keamanan antara Delhi dan Washington di Asia, Samudra Hindia dan sekitarnya, menuntut konsultasi substantif antara Delhi dan Washington.

12.8 KEAMANAN INFORMASI INTERNASIONAL (ORGANISASI KERJASAMA SHANGHAI)

Kesepakatan antara pemerintah negara-negara anggota organisasi kerjasama Shanghai tentang kerjasama di bidang memastikan keamanan informasi internasional (mulai 16 Juni 2009): Pemerintah negara-negara anggota organisasi kerjasama Shanghai (SCO) yang selanjutnya adalah disebut sebagai Pihak, Memperhatikan kemajuan yang signifikan dalam pengembangan dan penerapan teknologi informasi dan komunikasi terbaru dan sarana untuk menciptakan ruang informasi global, menyatakan keprihatinan dalam ancaman yang berhubungan dengan kemungkinan penggunaan teknologi dan sarana tersebut untuk tujuan, yang tidak sesuai dengan tugas-tugas untuk memastikan stabilitas dan keamanan internasional, yang berlaku baik untuk sipil, dan militer untuk bidang, memberikan pentingnya keamanan informasi internasional sebagai salah satu elemen penting dari sistem keamanan internasional, diyakinkan bahwa pendalaman lebih lanjut kepercayaan dan pengembangan interaksi Para Pihak dalam pertanyaan untuk memastikan keamanan informasi internasional adalah kebutuhan penting dan adil untuk kepentingan mereka, mempertimbangkan juga pentingnya peran keamanan informasi dalam memberikan hak dan kebebasan dasar manusia dan warga negara, mempertimbangkan rekomendasi dari resolusi Majelis Umum "Pencapaian di bidang informatisasi dan telekomunikasi dalam konteks keamanan internasional", bertujuan untuk membatasi ancaman keamanan informasi internasional, untuk memberikan kepentingan keamanan informasi Para Pihak dan untuk menciptakan lingkaran informasi internasional yang menjadi ciri dunia, kerjasama dan harmoni, yang ingin menciptakan dasar hukum dan organisasi kerjasama Para Pihak di bidang penyelenggaraan keamanan informasi internasional, disepakati sebagai berikut:

Pasal 1. Istilah dan konsep

Untuk tujuan interaksi Para Pihak dalam pemenuhan perjanjian ini, Daftar istilah dan konsep utama bidang memastikan keamanan informasi internasional menurut lampiran 1 perjanjian ini yang menjadi bagian integralnya akan digunakan.

Isi daftar istilah dan konsep ini dapat ditambahkan, ditentukan dan diperbarui sesuai kebutuhan sesuai kesepakatan.

Pasal 2. Ancaman utama di bidang keamanan informasi internasional

Mewujudkan kerja sama menurut kesepakatan Para Pihak ini dimulai dengan tersedianya ancaman-ancaman utama berikut di bidang penjaminan keamanan informasi internasional:

1. Pengembangan dan penggunaan senjata informasi, persiapan dan pelaksanaan perang informasi.
2. Terorisme informasi.
3. Kejahatan informasi.

12.9 INDIA PERLU MEMPERKUAT KEMAMPUAN KEAMANAN CYBERNYA

India sedang mencoba untuk mengimplementasikan proyek Digital India dengan kemampuan terbaiknya. Keberhasilan proyek Digital India akan bergantung pada konektivitas

maksimum dengan risiko keamanan siber minimum. Ini juga menjadi masalah bagi India karena India memiliki rekam jejak keamanan siber yang buruk. Misalnya, Komisi Telekomunikasi telah menyetujui layanan seluler berbasis satelit di India. Demikian pula, konektivitas nirkabel dan Internet gratis juga akan tersedia bagi orang-orang India untuk kenyamanan dan konektivitas yang lebih baik. Namun, ini akan meningkatkan keamanan nirkabel dan berbagai tantangan keamanan dunia maya juga. Meskipun Kebijakan Keamanan Cyber Nasional India 2013 (NCSP 2013) diumumkan oleh India seperti e-governance dan e-commerce masih berisiko dan mungkin memerlukan asuransi cyber dalam waktu dekat.

Serangan dunia maya telah meningkat pesat di seluruh dunia dan India juga diharuskan untuk melindungi perbatasan dunia mayanya melalui langkah-langkah hukum tekno. Pada saat yang sama, upaya harus dilakukan oleh India untuk merumuskan strategi pencegahan kejahatan dunia maya yang efektif dan memberikan pelatihan investigasi kejahatan dunia maya kepada lembaga penegak hukum India. Beberapa area spesifik yang perlu diperkuat oleh India untuk keamanan sibernya adalah perang siber, terorisme siber, spionase siber, perlindungan infrastruktur kritis (PDF), kerjasama keamanan siber internasional (PDF), dll. Di tingkat internasional, ada kecenderungan untuk memblokir aliran bebas teknologi keamanan siber. Baru-baru ini sebuah proposal diperdebatkan untuk memasukkan keamanan siber di bawah Pengaturan Wassenaar yang sangat menentang India. Jika diterima, pembatasan ekspor dapat diterapkan pada teknologi keamanan siber. India perlu memperkuat kemampuan keamanan sibernya yang harus mencakup kemampuan keamanan siber ofensif dan defensif. Kebijakan perang dunia maya India (PDF) juga harus segera dirumuskan yang harus mencakup tujuan pengembangan keterampilan keamanan dunia maya juga.

12.10 YAYASAN PERDAMAIAN CYBER

Dengan pertumbuhan internet dan penggunaan teknologi, dunia sedang mempersiapkan perang siber dengan mengangkat militer siber dan senjata sibernya sendiri. Telah tepat dikatakan bahwa perang dimensi kelima adalah CYBER WAR (sisanya 4 darat, laut, udara dan ruang angkasa), yang akan berdampak buruk pada keamanan informasi dunia. Tidak hanya itu, dapat mengakibatkan kekacauan total karena Infrastruktur Informasi Kritis dari negara-negara akan terpengaruh. Bidang kehidupan lain juga telah membawa risiko dan ancaman yang sangat besar terhadap perdamaian masyarakat siber. Setiap tindakan atau pemikiran diarahkan untuk mengendalikan hal-hal negatif yang disebarkan melalui media ini dan pada keamanan dunia maya. Di dunia saat ini, kejahatan dunia maya, penindasan dunia maya, perang dunia maya, terorisme dunia maya dan isu-isu anti-sosial semacam itu telah menjadi sangat menonjol. Dunia perlu menyadari fakta bahwa ada peran yang lebih besar untuk dimainkan dalam menggunakan media ini untuk menyebarkan dan mempromosikan Perdamaian.

Sudah saatnya kita mulai mengambil langkah-langkah keamanan siber proaktif dan juga menyuntikkan perdamaian ke dalam ekosistem siber. Mengingat hal ini, Cyber Peace Foundation (CPF) telah dibentuk dengan tujuan untuk membangun ruang cyber yang damai dan harmonis. Di antara sedikit organisasi di dunia yang bekerja untuk 'Perdamaian', CPF jelas merupakan LSM pertama di dunia yang bekerja untuk 'Perdamaian Cyber'. CPF berfokus pada kesadaran, konseling, pendidikan, pelatihan dan untuk menjangkau warga, pemerintah,

lembaga penegak hukum (LEA), perusahaan swasta, LSM yang bekerja di kejahatan dunia maya dan keamanan dunia maya, universitas, pakar keamanan dunia maya dan pemburu hadiah bug; untuk menyediakan platform bersama di tingkat global untuk SEMUA AHLI DI SATU JEMBATAN. Dalam upayanya untuk mengekang ancaman kejahatan dunia maya yang semakin meningkat dan mempromosikan keharmonisan dunia maya, CPF memiliki CYBER PEACE CORP. Kami bertindak sebagai titik kontak untuk berbagai pemerintah, LEA, dan sel dunia maya untuk memastikan penyelesaian damai dari setiap perselisihan terkait dunia maya. Tujuan organisasi adalah untuk memberdayakan semua melalui pengetahuan tentang ancaman, risiko dan peluang. CPF mengakui pentingnya konservasi ekosistem siber, sama seperti kita bekerja untuk melindungi lingkungan dunia nyata kita, dan sangat berkomitmen untuk tujuan ini.

12.11 RINGKASAN

Komunitas internasional mengembangkan konsensus tentang keamanan siber tetapi masih pada beberapa masalah tidak ada konsensus. Di unitnya konsep penting kebijakan keamanan siber AS, ancaman dan tantangan terhadap keamanan siber internasional, kerja sama internasional dan keamanan siber, Konvensi Uni Afrika tentang keamanan siber dan perlindungan data, Konvensi Dewan Eropa tentang Kejahatan Siber (Konvensi Budapest), pertahanan siber sensitivitas dalam perspektif India, keamanan informasi internasional, India perlu memperkuat kemampuan keamanan cybernya, dan Cyber Peace Foundation dibahas panjang lebar untuk pemahaman yang lebih baik dalam kepentingan untuk mengeksplorasi berbagai dimensi keamanan cyber.

12.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Authorpress)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew

- M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang tepat dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

12.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a Virus komputer Flame adalah program malware digital terbaru yang ditemukan dalam praktik peningkatan serangan dunia maya skala besar.

b Dunia maya menyentuh hampir setiap bagian dari kehidupan kita sehari-hari.

c Kami bekerja untuk mengembangkan tenaga kerja yang paham dunia maya dan pada akhirnya membuat dunia maya secara inheren lebih aman.

d Kurangnya kemitraan antara negara maju dan negara berkembang dapat menghasilkan "surga yang aman" bagi para penjahat dunia maya.

e Satu laporan internasional merekomendasikan pertukaran pandangan dan informasi tentang kebijakan nasional, praktik terbaik & lain-lain yang berkaitan dengan keamanan dunia maya.

B. Isi Bagian yang Kosong:

I. Sebuah.....ruang maya sangat penting bagi keberhasilan ekonomi global.

II. Menurut ....., ancaman terhadap dunia maya telah meningkat secara dramatis di masa lalu.

III. .....mewajibkan negara pihak untuk menetapkan kerangka hukum dan kelembagaan untuk perlindungan data dan keamanan siber.

IV. .....tentang kejahatan dunia maya adalah perjanjian internasional pertama yang bertujuan untuk menangani dan mengatasi kejahatan komputer.

V. India sedang mencoba untuk menerapkan ..... dengan kemampuan terbaiknya.

12.14. Jawaban untuk Memeriksa Kemajuan Anda:

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Terbuka, transparan, aman dan stabil

2. Studi Norton 2011
3. Konvensi Afrika
4. Konvensi Budapest
5. Proyek Digital India

12.15 PERTANYAAN TERMINAL

1. Apa itu Kebijakan Keamanan Siber AS?
2. Apa saja ancaman dan tantangan terhadap keamanan siber internasional?
3. Mendefinisikan kerjasama internasional dan keamanan siber.
4. Diskusikan Konvensi Uni Afrika tentang Keamanan Siber dan Perlindungan Data.
5. Bagaimana posisi India dalam keamanan pertahanan siber?

BAB 13
TERORISME CYBER: MAKNA, TANTANGAN, DAN ISU

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan International Treatise on Cyber Security
- Memahami sifat dan ruang lingkup Keamanan Siber di berbagai negara
- Memahami masalah teknis dan hukum terkait Keamanan Cyber

13.1 PENGANTAR

Terorisme dunia maya telah ada sejak akhir 1980-an namun jumlah terorisme internet hanya meningkat sejak serangan 11 September di Amerika Serikat. Beberapa contoh kegiatan terorisme dunia maya termasuk pengeboman email, peretasan ke portal pemerintah, situs web perbankan, air, dan rumah sakit untuk menimbulkan ketakutan atau membahayakan nyawa banyak orang. Beberapa contoh serangan terorisme dunia maya sebelumnya adalah pada tahun 1996 ketika seorang peretas komputer yang mengaku terkait dengan gerakan White Supremacist untuk sementara menonaktifkan dan merusak Penyedia Layanan Internet Massachusetts (ISP) sementara ia mengirimkan pesan rasis ke seluruh dunia dengan nama ISP. Sementara pada tahun 1999, selama konflik Kosovo, komputer North Atlantic Treaty Organization (NATO) diledakkan dengan bom email dan dipukul dengan serangan Denial-of-Service (DoS) oleh peretas yang memprotes pemboman NATO. Baru-baru ini, pada tahun 2000, seseorang menyusup ke Maroochy Shire, sistem pengendalian pengelolaan limbah Australia dan melepaskan jutaan galon limbah mentah di kota tersebut. Seiring dengan meningkatnya pengetahuan tentang penggunaan internet, tren telah bergeser dan teroris menggunakan dunia maya untuk memfasilitasi metode terorisme yang lebih tradisional seperti pengeboman atau menyebarkan pesan kebencian. Situs web kelompok teroris khususnya digunakan untuk menyajikan pesan, mengoordinasikan anggota, dan merekrut pendukung muda. Beberapa situs web ini juga didirikan sebagai sumber pembiayaan kegiatan mereka melalui penjualan barang dagangan mereka. Negara-negara seperti Amerika Serikat dan di benua Eropa dan negara-negara Asia yang kuat seperti Cina dan India telah mengambil tindakan pencegahan mereka sendiri dalam memerangi terorisme dunia maya.

13.2 CYBER TERRORISM-ARTI

Menurut Biro Investigasi Federal A.S., terorisme cyber adalah "serangan terencana, bermotivasi politik terhadap informasi, sistem komputer, program komputer, dan data yang mengakibatkan kekerasan terhadap target non-pejuang oleh kelompok sub-nasional atau Agen rahasia Menurut U.S. Federal Bureau of Investigation, cyber terrorism adalah "serangan terencana, bermotivasi politik terhadap informasi, sistem komputer, program komputer, dan data yang menghasilkan kekerasan terhadap target non-kombatan oleh kelompok sub-nasional atau agen klandestin. ." Tidak seperti virus pengganggu atau serangan komputer yang mengakibatkan penolakan layanan, serangan teroris dunia maya dirancang untuk

menyebabkan kekerasan fisik atau kerugian finansial yang ekstrem. Menurut Komisi Perlindungan Infrastruktur Kritis A.S., kemungkinan target teroris dunia maya termasuk industri perbankan , instalasi militer, pembangkit listrik, pusat kontrol lalu lintas udara, dan sistem air. Terorisme dunia maya kadang-kadang disebut sebagai terorisme elektronik atau perang informasi.

Setelah serangan komputer baru-baru ini, banyak yang dengan cepat mengambil kesimpulan bahwa jenis terorisme baru sedang meningkat dan negara kita harus mempertahankan diri dengan segala cara yang mungkin. Sebagai masyarakat, kita memiliki pengalaman operasional dan hukum yang luas serta teknik yang terbukti untuk memerangi terorisme, tetapi apakah kita siap untuk memerangi terorisme di arena baru – ruang siber? Rencana strategis operasi tempur mencakup karakterisasi tujuan musuh, teknik operasional, sumber daya, dan agen. Sebelum mengambil tindakan agresif di bidang legislatif dan operasional, kita harus mendefinisikan musuh dengan tepat. Artinya, definisi terorisme harus diperluas hingga mencakup terorisme siber. Sebagai masyarakat yang membanggakan ketidakberpihakan keadilan, kita harus memberikan pedoman legislatif yang jelas dan definitif untuk menangani terorisme jenis baru. Seperti yang terjadi sekarang, keadilan tidak dapat ditegakkan karena kami belum memberikan definisi yang jelas tentang istilah tersebut. Dalam hal ini, saya mengusulkan untuk memeriksa kembali pemahaman kita tentang terorisme cyber.

Ada banyak salah tafsir dalam definisi cyber-terrorism, kata yang terdiri dari "cyber" yang akrab dan "terorisme" yang kurang akrab. Sementara "cyber" adalah segala sesuatu yang berhubungan dengan alat perdagangan kita, terorisme pada dasarnya sulit untuk didefinisikan. Bahkan pemerintah AS tidak dapat menyetujui satu definisi tunggal. Pepatah lama, "Teroris satu orang adalah pejuang kemerdekaan orang lain" masih hidup dan sehat.

Ambiguitas dalam definisi membawa ketidakjelasan dalam tindakan, seperti yang ditunjukkan D. Denning dalam karyanya Activism, Hactivism and Cyber terrorism, "sebuah bom email dapat dianggap hacktivism oleh beberapa orang dan cyber-terrorism oleh orang lain". Oleh karena itu, ada tingkat "pemahaman" tentang arti terorisme cyber, baik dari media populer, sumber sekunder lainnya, atau pengalaman pribadi; namun, para ahli menggunakan definisi makna yang berbeda. Cyber-terorisme serta "terorisme" kontemporer lainnya (bioterorisme, terorisme kimia, dll.) muncul sebagai campuran kata terorisme dan makna area aplikasi. Barry Collin, seorang peneliti senior di Institut Keamanan dan Intelijen di California, yang pada tahun 1997 dikaitkan dengan penciptaan istilah "Terorisme siber", mendefinisikan terorisme siber sebagai konvergensi sibernetika dan terorisme. Pada tahun yang sama Mark Pollitt, agen khusus untuk FBI, menawarkan definisi kerja: "Terorisme siber adalah serangan yang direncanakan, bermotivasi politik terhadap informasi, sistem komputer, program komputer, dan data yang mengakibatkan kekerasan terhadap target non-kombatan oleh kelompok sub-nasional atau agen rahasia."

Sejak saat itu kata cyber-terrorism telah masuk ke dalam leksikon spesialis keamanan TI dan ahli teroris dan daftar kata media massa "profesional". Salah satu ahli, seorang kepala polisi, menawarkan versi definisinya: "Terorisme siber – menyerang target yang rawan sabotase oleh komputer – berpotensi menimbulkan konsekuensi bencana bagi masyarakat kita yang sangat bergantung pada komputer."

Media sering menggunakan istilah terorisme cyber dengan sengaja: "Bocah Kanada mengakui terorisme cyber keluarganya: "Emeryville, Ontario (Reuter) - Seorang bocah lelaki Kanada berusia 15 tahun telah mengakui bahwa dia bertanggung jawab atas lelucon teknologi tinggi yang terkenal selama berbulan-bulan yang meneror keluarganya sendiri, kata polisi Senin". Seorang pakar terkenal Dorothy Denning mendefinisikan terorisme siber sebagai "serangan dan ancaman yang melanggar hukum terhadap komputer, jaringan, dan informasi yang tersimpan di dalamnya ketika dilakukan untuk mengintimidasi atau memaksa pemerintah atau rakyatnya untuk melanjutkan tujuan politik atau sosial". R. Stark dari Universitas SMS mendefinisikan terorisme dunia maya sebagai "serangan apa pun terhadap fungsi informasi, apa pun caranya". Berdasarkan definisi terorisme dunia maya yang disebutkan di atas, orang hanya dapat menunjukkan fakta bahwa setiap serangan infrastruktur telekomunikasi, termasuk perusakan situs dan lelucon komputer lainnya, merupakan terorisme, artinya terorisme dunia maya telah terjadi dan kita "hidup" di zaman teror dunia maya.

Namun, ahli lain, James Christy, koordinator penegakan hukum dan kontra intelijen untuk DIAP (Program Jaminan Informasi Pertahanan), yang dipimpin oleh kantor asisten menteri pertahanan untuk komando, kontrol, komunikasi dan intelijen, menyatakan bahwa cyber- terorisme tidak pernah dilancarkan terhadap Amerika Serikat. “Sebaliknya, peristiwa peretasan baru-baru ini – termasuk halaman web tahun 1998 yang dibuat oleh pendukung kelompok pemberontak Zapatistas Meksiko, yang menyebabkan serangan terhadap militer AS dari 1.500 lokasi di 50 negara berbeda – merupakan kejahatan komputer. William Church, mantan pejabat AS. Perwira Intelijen Angkatan Darat, yang mendirikan Center for Infrastructural Warfare Studies (CIWARS) setuju bahwa Amerika Serikat belum melihat ancaman teroris cyber dari teroris menggunakan teknik perang informasi. melawan infrastruktur" Richard Clarke, koordinator nasional untuk keamanan, perlindungan infrastruktur dan kontraterorisme di Dewan Keamanan Nasional menawarkan untuk berhenti menggunakan "terorisme dunia maya" dan menggunakan "perang informasi" sebagai gantinya.

Pengamatan yang disebutkan di atas mendorong garis yang jelas antara terorisme siber dan kejahatan siber dan memungkinkan kita untuk mendefinisikan terorisme siber sebagai: Penggunaan teknologi informasi dan sarana oleh kelompok dan agen teroris. Dalam mendefinisikan aktivitas cyber teroris, perlu dilakukan segmentasi aksi dan motivasi. Tidak ada keraguan bahwa tindakan peretasan dapat memiliki konsekuensi yang sama dengan tindakan terorisme tetapi dalam pengertian hukum penyalahgunaan informasi dunia maya yang disengaja harus menjadi bagian dari kampanye atau tindakan teroris. Contoh aktivitas teroris dunia maya dapat mencakup penggunaan teknologi informasi untuk mengatur dan melakukan serangan, aktivitas kelompok pendukung, dan kampanye manajemen persepsi. Para ahli sepakat bahwa banyak kelompok teroris seperti organisasi Osama bin Ladenn dan kelompok militan Islam Hamas telah mengadopsi teknologi informasi baru sebagai sarana untuk melakukan operasi tanpa terdeteksi oleh pejabat kontra teroris. Dengan demikian, penggunaan teknologi informasi dan sarana oleh kelompok dan agen teroris merupakan terorisme siber. Kegiatan lain, yang begitu diagungkan oleh media, harus didefinisikan sebagai kejahatan dunia maya.

13.3 JENIS-JENIS TERORISME DUNIA MAYA

Jejaring sosial melalui Internet telah berkembang pesat dalam beberapa tahun terakhir karena memungkinkan jaringan individu yang berpikiran sama untuk berkolaborasi dan terhubung, terlepas dari geografi atau lokasi fisik mereka masing-masing. Terorisme dunia maya sebagaimana disebutkan adalah masalah yang sangat serius dan mencakup berbagai macam serangan.

Beberapa alat utama kejahatan dunia maya mungkin- Botnets, Estonia, 2007, Kode Berbahaya yang Dihosting di Situs Web, Spionase Cyber dll. Penting untuk menandai di sini bahwa ada bentuk lain yang dapat dicakup di bawah judul Kejahatan Dunia Maya & secara bersamaan juga merupakan alat penting untuk kegiatan teroris. Di sini saya akan membahas kegiatan kriminal ini satu per satu: Serangan melalui Internet : Akses tidak sah & Peretasan: salah satu kegiatan kriminal adalah akses tidak sah yang berarti segala jenis akses tanpa izin dari pemilik yang sah atau orangnya penanggung jawab komputer, sistem komputer, atau jaringan komputer Setiap tindakan yang dilakukan untuk membobol komputer dan/atau jaringan adalah peretasan. Hacker menulis atau menggunakan program komputer yang sudah jadi untuk menyerang komputer target. Mereka memiliki keinginan untuk merusak dan mereka mendapatkan tendangan dari kehancuran tersebut. Serangan Trojan: Trojan adalah program yang bertindak seperti sesuatu yang berguna tetapi melakukan hal-hal yang redaman yang tenang. Program semacam ini disebut sebagai Trojan. Trojan datang dalam dua bagian, bagian Klien dan bagian Server.

Ketika korban (tanpa sadar) menjalankan server pada mesinnya, penyerang kemudian akan menggunakan Klien untuk terhubung ke Server dan mulai menggunakan Trojan Virus dan serangan Worm: Sebuah program yang memiliki kemampuan untuk menginfeksi program lain dan membuat salinan dari dirinya sendiri dan menyebar ke program lain disebut virus. Program yang berkembang biak seperti virus tetapi menyebar dari komputer ke komputer disebut sebagai worm. Kejahatan terkait email: Email spoofing: Email spoofing mengacu pada email yang tampaknya berasal dari satu sumber padahal sebenarnya dikirim dari sumber lain.2. Email Spamming Email "spamming" mengacu pada pengiriman email ke ribuan dan ribuan pengguna - mirip dengan surat berantai. Mengirim kode berbahaya melalui email E-mail digunakan untuk mengirim virus, Trojan, dll melalui email sebagai lampiran atau dengan mengirimkan tautan situs web yang sedang dikunjungi untuk mengunduh kode berbahaya.

Setelah penyelidikan tentang berbagai jenis terorisme Cyber yang mungkin terjadi pada siapa saja atau organisasi, saya ingin menyebutkan beberapa studi kasus untuk menunjukkan definisi dan teori ini dalam kehidupan nyata.

Seperti yang Anda ketahui, salah satu bentuk terorisme Cyber yang paling populer adalah mengancam bank besar. Para teroris meretas sistem dan kemudian meninggalkan pesan terenkripsi untuk direktur senior, yang mengancam bank. Apa yang menambah kesulitan untuk menangkap penjahat adalah bahwa penjahat mungkin berada di negara lain. Kesulitan kedua adalah bahwa sebagian besar bank lebih suka membayar uang daripada membuat publik tahu betapa rentannya mereka.

13.4 PENGARUH TERORISME CYBER TERHADAP INFRASTRUKTUR NASIONAL/INTERNASIONAL

Maksud serangan terorisme siber dapat berkisar dari gangguan ekonomi melalui gangguan jaringan dan sistem keuangan atau digunakan untuk mendukung serangan fisik hingga menyebabkan kebingungan lebih lanjut dan kemungkinan penundaan dalam respons yang tepat. Meskipun serangan siber telah menyebabkan kerugian miliaran dolar dan mempengaruhi kehidupan jutaan orang, kita belum menyaksikan implikasi dari serangan terorisme siber yang benar-benar dahsyat. Apa beberapa implikasinya? Implikasi Biaya Langsung

- Kehilangan penjualan selama gangguan
- Waktu staf, penundaan jaringan, akses terputus-putus untuk pengguna bisnis
- Peningkatan biaya asuransi karena litigasi
- Hilangnya kekayaan intelektual – penelitian, penetapan harga, dll.
- Biaya forensik untuk pemulihan dan litigasi
- Hilangnya komunikasi penting pada saat darurat
- Implikasi Biaya Tidak Langsung
- Hilangnya kepercayaan dan kredibilitas dalam sistem keuangan kita
- Hubungan yang ternoda & citra publik secara global
- Hubungan mitra bisnis yang tegang – domestik dan internasional
- Hilangnya pendapatan pelanggan di masa depan untuk individu atau kelompok perusahaan
- Hilangnya kepercayaan pada pemerintah dan industri komputer

Undang-undang baru mengharuskan pelanggaran sistem untuk dilaporkan (SB1386 California). Undang-undang lain yang diusulkan akan memungkinkan ganti rugi dicari oleh korban serangan yang diluncurkan dari sistem web yang diretas. SB 1386 California adalah tindakan menyeluruh yang mengamanatkan pengungkapan publik tentang pelanggaran keamanan komputer di mana informasi rahasia dari setiap penduduk California mungkin telah dikompromikan. RUU tersebut selanjutnya mendefinisikan informasi pribadi sebagai nama depan atau inisial dan nama belakang individu dalam kombinasi dengan SSN, nomor SIM, atau nomor rekening, nomor kartu kredit, nomor kartu debit, dan kata sandi atau kode terkait. Pikirkan tanggung jawab yang akan ditanggung organisasi jika sistem mereka disusupi dan ribuan informasi pribadi individu diekspos dan bahkan dieksploitasi untuk keuntungan finansial – (mendanai terorisme).

Dengan virus "LoveBug" yang menelan biaya hampir Rp 150.000 miliar, sulit untuk memahami implikasi keuangan dari serangan yang jauh lebih serius dan komprehensif. Setiap hari perusahaan di AS dan luar negeri menghabiskan jutaan dolar untuk memerangi ancaman serangan dunia maya dan terorisme dunia maya. Upaya perusahaan mencapai puluhan (jika bukan ratusan) miliaran dolar setiap tahun dan dengan meningkatnya frekuensi serangan, biayanya akan meningkat secara signifikan di tahun-tahun mendatang. Saat kita menghadapi serangan yang semakin kompleks dari pejuang cyber profesional, perusahaan akan semakin mencari bantuan dari pemerintah di seluruh dunia untuk menggagalkan upaya ini dan membendung pendarahan keuangan.

13.5 KARAKTERISTIK TERORISME CYBER

"Kapan serangan di dunia maya dianggap sebagai terorisme? Pertanyaan tersebut dapat dijawab dengan meneliti apa saja elemen umum dari semua terorisme. Menurut Vatis (2001.) tindakan terorisme adalah:

- direncanakan dan bukan hanya tindakan yang lahir dari kemarahan,
- politik dan dirancang untuk mempengaruhi struktur politik,
- ditargetkan pada warga sipil dan instalasi sipil, dan
- dilakukan oleh kelompok ad hoc sebagai lawan dari tentara nasional.

Ketika elemen-elemen ini diterapkan pada terorisme dunia maya, tampaknya tidak ada satupun yang gagal. Pertama, serangan teroris cyber direncanakan dan harus direncanakan karena melibatkan pengembangan atau akuisisi perangkat lunak untuk melakukan serangan. Kedua, tindakan terorisme dunia maya dimaksudkan untuk merusak/menghancurkan sepenuhnya suatu sistem atau sistem komputer (Galley 1996.). Teroris dunia maya adalah peretas dengan motivasi politik, serangan mereka dapat berdampak pada struktur politik melalui korupsi dan perusakan ini (Furnell dan Warren1999, 30.) Ketiga, serangan teroris dunia maya sering menargetkan kepentingan sipil. Denning mengkualifikasikan terorisme cyber sebagai serangan yang mengakibatkan kekerasan terhadap orang atau properti, atau setidaknya menyebabkan kerusakan yang cukup untuk menimbulkan ketakutan (Denning 2000a.). Keempat, terorisme dunia maya terkadang dibedakan dari perang dunia maya, yaitu serangan berbasis komputer yang diatur oleh agen negara-bangsa."

13.6 TERORISME CYBER-TANTANGAN DAN MASALAH

Memahami mengapa, bagaimana dan dengan konsekuensi apa teroris dapat dan ingin menggunakan domain siber untuk tujuan mereka sangat penting untuk merumuskan praktik kebijakan terbaik dalam mencegah dan mengelola munculnya 'komunitas' teroris yang diberdayakan siber. Analisis wacana, epistemologi dan teori perang Sun Tzu, bersama dengan konsep-konsep terkait lainnya dari dunia maya hubungan internasional.

Perkembangan teknologi telah melihat domain virtual berkembang secara dramatis, dan abad ke-21 menandai percepatan di dunia online dan ancaman yang muncul darinya. Beberapa tahun terakhir memiliki pengalaman tidak hanya peningkatan akses ke internet di seluruh dunia, kemampuan program yang lebih besar dan jangkauan layanan yang lebih luas. Komputer juga membawa masalah teknis, politik, sosial dan ekonomi, dengan malware yang lahir pada frekuensi yang lebih tinggi daripada obat untuk itu.

Kontrol atas target dan penyerang menjadi sangat sulit untuk dicapai; dan yang terakhir- praktis tidak mungkin. Kecenderungan peretasan yang lebih rumit dan kompleks sering menargetkan objek penting - pribadi dan publik. Meskipun untuk saat ini, dunia maya menjadi domain yang sangat diperhatikan dalam hubungan antar negara, potensi kelompok teroris mengembangkan kemampuan, akses dan motivasi untuk menargetkan Negara dan, memang, infrastruktur swasta sangat serius. Banyak laporan, penelitian dan informasi intelijen yang dikumpulkan menunjukkan bahwa dalam beberapa tahun dari sekarang, teroris dapat memperoleh keterampilan yang cukup untuk menggunakan ruang siber untuk tujuan serangan (Aitoro, 2009; GCN, 2012; Guneev, 2012).

Subyek terorisme dunia maya terletak dalam bidang penelitian yang sangat baru; oleh karena itu publikasi khusus sangat terbatas. Namun, diposisikan dalam konteks yang lebih luas, penelitian dengan mudah tumpang tindih dengan banyak disiplin ilmu, dan ini akan dieksplorasi secara rinci. Penulis, doktrin, pemerintah, dan organisasi internasional berbeda pendapat tidak hanya mengenai apakah terorisme dunia maya itu mungkin, tetapi juga tentang konsekuensinya, jika dianggap sebagai situasi yang masuk akal. Saya akan memberikan gambaran singkat tentang garis pemikiran yang berlaku saat ini. Kontroversi dalam literatur sebagian besar didasarkan pada ketidakmungkinan untuk mendefinisikan dengan tepat istilah-istilah dan menyesuaikannya dengan undang-undang yang ada atau ke dalam kebijakan negara tentang perang dunia maya.

13.7 SIAPA TERORIS CYBER?

Seorang programmer yang membobol sistem komputer untuk mencuri atau mengubah atau menghancurkan informasi sebagai bentuk terorisme cyber. Dari sudut pandang Amerika, kelompok teroris paling berbahaya adalah Al-Qaeda yang dianggap sebagai musuh pertama AS. Accor^iha ni US i``i]i[f‖m ^[n[dari komputer yang disita di Afghanistan menunjukkan bahwa kelompok tersebut telah mengintai sistem yang mengontrol fasilitas energi Amerika, distribusi air, sistem komunikasi, dan infrastruktur penting lainnya. Setelah April 2001 tabrakan pesawat mata-mata angkatan laut AS dan jet tempur China, hacker China meluncurkan serangan Denial so Service (DoS) terhadap situs web Amerika.

Sebuah studi yang mencakup paruh kedua tahun 2002 menunjukkan bahwa negara paling berbahaya untuk memulai serangan cyber berbahaya adalah Amerika Serikat dengan 35,4% kasus turun dari 40% untuk paruh pertama tahun yang sama. Korea Selatan datang berikutnya dengan 12,8%, diikuti oleh Cina 6,2% kemudian Jerman 6,7% kemudian Prancis 4%. Inggris datang nomor 9 dengan 2,2%. Menurut penelitian yang sama, Israel adalah negara paling aktif dalam hal jumlah serangan dunia maya terkait dengan jumlah pengguna internet. Ada begitu banyak kelompok yang sangat aktif menyerang target mereka melalui komputer. Unix Security Guards (USG) sebuah kelompok pro Islam meluncurkan banyak serangan digital pada Mei 2002. Kelompok lain yang disebut World's Fantabulas Defacers (WFD) menyerang banyak situs India. Juga ada kelompok pro Pakistan lainnya yang disebut Anti India Crew (AIC) yang melancarkan banyak serangan cyber terhadap India. Ada begitu banyak kelompok Palestina dan Israel yang saling berperang melalui serangan digital.

13.8 SERANGAN KOMPUTER DAN TERORISME CYBER

Serangan komputer dapat didefinisikan sebagai tindakan yang diarahkan terhadap sistem komputer untuk mengganggu operasi peralatan, mengubah kontrol pemrosesan, atau merusak data yang disimpan. Metode serangan yang berbeda menargetkan kerentanan yang berbeda dan melibatkan berbagai jenis senjata, dan beberapa mungkin berada dalam kemampuan saat ini dari beberapa kelompok teroris. Tiga metode serangan yang berbeda diidentifikasi dalam laporan ini, berdasarkan efek dari senjata yang digunakan. Namun, seiring berkembangnya teknologi, perbedaan antara metode ini mungkin mulai kabur.

- Serangan fisik melibatkan senjata konvensional yang diarahkan ke fasilitas komputer atau jalur transmisinya;

- Sebuah serangan elektronik (EA) melibatkan penggunaan kekuatan energi elektromagnetik sebagai senjata, lebih umum sebagai pulsa elektromagnetik (EMP) untuk membebani sirkuit komputer, tetapi juga dalam bentuk yang lebih ringan, untuk memasukkan aliran berbahaya kode digital langsung ke transmisi radio gelombang mikro musuh; dan
- Serangan jaringan komputer (CNA), biasanya melibatkan kode berbahaya yang digunakan sebagai senjata untuk menginfeksi komputer musuh untuk mengeksploitasi kelemahan dalam perangkat lunak, dalam konfigurasi sistem, atau dalam praktik keamanan komputer dari suatu organisasi atau pengguna komputer. Bentuk lain dari CNA diaktifkan ketika penyerang menggunakan informasi curian untuk memasuki sistem komputer yang dibatasi.

Pejabat DOD telah menyatakan bahwa sementara ancaman CNA dan EA "lebih kecil kemungkinannya" daripada serangan fisik, mereka sebenarnya bisa terbukti lebih merusak karena melibatkan teknologi pengganggu yang mungkin menghasilkan konsekuensi yang tidak terduga atau memberikan keuntungan tak terduga bagi musuh. Karakteristik Serangan Fisik: Serangan fisik mengganggu keandalan peralatan komputer dan ketersediaan data. Serangan fisik diimplementasikan baik melalui penggunaan senjata konvensional, menciptakan panas, ledakan, dan fragmentasi, atau melalui manipulasi langsung kabel atau peralatan, biasanya setelah mendapatkan akses fisik yang tidak sah.

Pada tahun 1991, selama Operasi Badai Gurun, militer AS dilaporkan mengganggu komunikasi Irak dan pusat komputer dengan mengirimkan rudal jelajah untuk menyebarkan filamen karbon yang menyebabkan hubungan arus pendek jalur catu daya. Juga, serangan Al Qaeda yang ditujukan terhadap World Trade Center dan Pentagon pada 11 September 2001, menghancurkan banyak database komputer penting dan mengganggu sistem keuangan dan komunikasi sipil dan militer yang terhubung secara global. Hilangnya sementara tautan komunikasi dan data penting menambah efek serangan fisik dengan menutup pasar keuangan hingga seminggu.

Karakteristik Serangan Elektronik (EA): Serangan elektronik, paling sering disebut sebagai Pulsa Elektromagnetik (EMP), mengganggu keandalan peralatan elektronik melalui pembangkitan energi tinggi seketika yang membebani papan sirkuit, transistor, dan elektronik lainnya. Efek EMP dapat menembus dinding fasilitas komputer di mana mereka dapat menghapus memori elektronik, merusak perangkat lunak, atau menonaktifkan semua komponen elektronik secara permanen. Beberapa menegaskan bahwa sedikit yang telah dilakukan oleh sektor swasta untuk melindungi terhadap ancaman dari pulsa elektromagnetik, dan bahwa sistem elektronik komersial di Amerika Serikat dapat rusak parah oleh jangkauan terbatas, skala kecil, atau perangkat pulsa elektromagnetik portabel. Beberapa ahli militer telah menyatakan bahwa Amerika Serikat mungkin adalah negara yang paling rentan terhadap serangan pulsa elektromagnetik.

Sebuah Komisi untuk Menilai Ancaman dari Pulsa Elektromagnetik Ketinggian didirikan oleh Kongres pada TA2001 setelah beberapa ahli menyatakan keprihatinan bahwa Infrastruktur dan militer penting AS rentan terhadap serangan EMP ketinggian tinggi. Pada sidang 22 Juli 2004 di hadapan House Armed Services Committee, anggota panel dari Komisi dilaporkan menyatakan bahwa semakin banyak senjata militer AS dan sistem kontrol menjadi

semakin kompleks, mereka mungkin juga lebih rentan terhadap efek EMP. Konsensus Komisi adalah bahwa serangan EMP ketinggian tinggi skala besar mungkin dapat membuat masyarakat kita dalam bahaya yang serius dan dapat mengakibatkan kekalahan pasukan militer kita.

Namun, Departemen Keamanan Dalam Negeri (DHS) telah menyatakan bahwa pengujian generasi saat ini dari sakelar telekomunikasi inti sipil yang sekarang digunakan telah menunjukkan bahwa sakelar tersebut hanya sedikit terpengaruh oleh EMP. DHS juga telah menyatakan bahwa sebagian besar aset komunikasi inti untuk Amerika Serikat ditempatkan di fasilitas besar yang dibangun dengan sangat baik yang memberikan ukuran perlindungan terhadap efek EMP.

Pengamat percaya bahwa memasang serangan terkoordinasi terhadap komputer AS sistem, baik menggunakan senjata EMP skala besar, skala kecil, atau bahkan portabel memerlukan keterampilan teknis yang berada di luar kemampuan sebagian besar organisasi teroris. Namun, negara-negara seperti Rusia, dan mungkin negara-negara yang mensponsori teroris seperti Korea Utara, sekarang memiliki kemampuan teknis untuk membangun dan menggunakan perangkat EMP yang digerakkan oleh bahan kimia atau baterai yang lebih kecil yang dapat mengganggu komputer pada jangkauan terbatas.

Karakteristik serangan Cyber (CNA): Sebuah serangan jaringan komputer (CNA), atau "serangan cyber," mengganggu integritas atau keaslian data, biasanya melalui kode berbahaya yang mengubah logika program yang mengontrol data, menyebabkan kesalahan dalam output (untuk lebih detail, lihat Lampiran A, B, dan C). Peretas komputer secara oportunis memindai Internet mencari sistem komputer yang salah konfigurasi atau tidak memiliki perangkat lunak keamanan yang diperlukan. Setelah terinfeksi kode berbahaya, komputer dapat dikendalikan dari jarak jauh oleh peretas yang mungkin, melalui Internet, mengirim perintah untuk memata-matai konten komputer itu atau menyerang dan mengganggu komputer lain.

Serangan dunia maya biasanya mengharuskan komputer yang ditargetkan memiliki beberapa kelemahan sistem yang sudah ada sebelumnya, seperti kesalahan perangkat lunak, kurangnya perlindungan antivirus, atau konfigurasi sistem yang salah, agar kode berbahaya dapat dieksploitasi. Namun, seiring perkembangan teknologi, persyaratan CNA yang membedakan ini mungkin mulai memudar. Misalnya, beberapa bentuk EA sekarang dapat menyebabkan efek yang hampir identik dengan beberapa bentuk CNA. Misalnya, pada tingkat daya yang terkendali, transmisi antara menara radio gelombang mikro yang ditargetkan dapat dibajak dan virus yang dirancang khusus, atau kode yang diubah, dapat dimasukkan langsung ke jaringan digital musuh.

13.9 TUJUH JENIS MOTIVASI HACKER

Ada hacker yang baik dan jahat. Berikut adalah jendela tentang apa yang mereka lakukan dan mengapa:

White Hat Hacker: Ini adalah orang-orang baik, pakar keamanan komputer yang berspesialisasi dalam pengujian penetrasi dan metodologi lain untuk memastikan bahwa sistem informasi perusahaan aman. Para profesional keamanan TI ini mengandalkan gudang teknologi yang terus berkembang untuk memerangi peretas.

Peretas Black Hat: Ini adalah orang-orang jahat, yang biasanya disebut sebagai peretas biasa. Istilah ini sering digunakan khusus untuk hacker yang membobol jaringan atau komputer, atau membuat virus komputer. Peretas topi hitam terus melampaui teknologi topi putih. Mereka sering berhasil menemukan jalan yang paling tidak tahan, baik karena kesalahan manusia atau kemalasan, atau dengan jenis serangan baru. Hacking puritan sering menggunakan istilah "cracker" untuk merujuk pada peretas topi hitam. Motivasi topi hitam umumnya untuk mendapatkan bayaran.

Script Kiddies: Ini adalah istilah menghina untuk peretas topi hitam yang menggunakan program pinjaman untuk menyerang jaringan dan merusak situs web dalam upaya membuat nama untuk diri mereka sendiri.

Hacktivists: Beberapa aktivis hacker termotivasi oleh politik atau agama, sementara yang lain mungkin ingin mengekspos kesalahan, atau membalas dendam, atau hanya melecehkan target mereka untuk hiburan mereka sendiri.

Peretas yang Disponsori Negara: Pemerintah di seluruh dunia menyadari bahwa itu melayani tujuan militer mereka untuk diposisikan dengan baik secara online. Pepatah dulu adalah, "Dia yang mengendalikan dunia." Tidak, ini semua tentang mengendalikan dunia maya. Peretas yang disponsori negara memiliki waktu dan dana tanpa batas untuk menargetkan warga sipil, perusahaan, dan pemerintah.

Peretas Mata-Mata: Perusahaan mempekerjakan peretas untuk menyusup ke kompetisi dan mencuri rahasia dagang. Mereka mungkin meretas dari luar atau mendapatkan pekerjaan untuk bertindak sebagai tahi lalat. Peretas mata-mata dapat menggunakan taktik yang sama dengan peretas, tetapi satu-satunya agenda mereka adalah melayani tujuan klien mereka dan mendapatkan bayaran.

Teroris Cyber: Peretas ini, umumnya dimotivasi oleh keyakinan agama atau politik, berusaha menciptakan ketakutan dan kekacauan dengan mengganggu infrastruktur penting. Teroris dunia maya sejauh ini adalah yang paling berbahaya, dengan berbagai keterampilan dan tujuan. Motivasi utama Teroris Cyber adalah untuk menyebarkan ketakutan, teror dan melakukan pembunuhan.

13.10 STRATEGI MENGHADAPI ANCAMAN TERORISME DUNIA MAYA

Berurusan dengan teroris dunia maya dan terorisme dunia maya membutuhkan rencana yang matang dan matang, dan kemauan untuk mengambil tindakan segera, sebaiknya sebelum peristiwa teroris terjadi. Berikut ini adalah pendekatan sederhana untuk keamanan siber:

1. Lakukan apa pun untuk melindungi infrastruktur.
2. Berinvestasi untuk melindungi produk Anda.
3. Lindungi klien Anda, termasuk data pribadi mereka.

Pastikan infrastruktur Anda, baik itu komputer pribadi, media sosial, dan akun online Anda atau stasiun saluran air bernilai miliaran dolar dilindungi. Mulai dari yang kecil. Pastikan semua kata sandi kuat dengan memasukkan huruf kapital dan huruf kecil, angka dan simbol dalam kombinasi yang tidak biasa. Investasikan pada produk yang meningkatkan keamanan sistem, seperti perlindungan malware dan deteksi virus, serta gunakan enkripsi untuk membantu melindungi informasi pribadi klien Anda.

Mengambil keamanan ke tingkat yang lebih tinggi, pertimbangkan untuk menyewa peretas etis untuk mencoba mendapatkan akses ke sistem Anda, dan segera menambal kerentanan apa pun. Juga pertimbangkan pemantauan ancaman orang dalam untuk mengidentifikasi perilaku dan anomali dengan sistem Anda dan untuk membantu memenuhi tuntutan sumber daya manusia. Dibutuhkan banyak orang untuk melindungi organisasi secara memadai, sama seperti dibutuhkan banyak orang untuk menyelesaikan serangan cyber. Karena itu, berpikirlah seperti teroris dunia maya untuk mengalahkan mereka di permainan mereka sendiri. Mereka menggunakan teknologi untuk mencapai tujuan teroris mereka, jadi ikuti dan gunakan teknologi etis untuk memerangi tindakan tidak etis mereka dan sebarkan keamanan sejauh mungkin di dalam organisasi Anda.

Selamat dari Terorisme Siber

Melawan teroris siber yang sangat canggih dan cerdas tampaknya merupakan situasi yang tidak menguntungkan, tetapi dengan teknologi yang tepat, para ahli, dan kemauan untuk merespons, eksploitasi dapat diminimalkan.

Langkah-langkah berikut mengajarkan Anda apa yang harus dilakukan sebelum, selama dan setelah serangan terorisme cyber.

1. Antisipasi serangan siber: Pertanyaannya bukan apakah teroris siber akan menyerang, tapi kapan. Pikirkan tentang strategi pencegahan dan apa yang dapat Anda lakukan sekarang. Jangan menunggu sampai Anda diserang untuk melakukan sesuatu karena itu akan terlambat.
2. Segera tanggapi untuk meningkatkan kelangsungan bisnis: Saat diserang, tujuannya adalah untuk menjaga agar bisnis berfungsi sebagai unit yang kohesif setiap saat. Ini dimungkinkan jika Anda telah menetapkan rencana keamanan Anda dan telah mempraktekkan apa yang harus dilakukan sebelum serangan muncul kembali.
3. Pantau semua sistem secara real time: Investasikan teknologi dan pakar untuk memantau sistem Anda 24 jam sehari, 7 hari seminggu, 365 hari setahun.
4. Evolve: Jangan pernah berhenti belajar cara bertahan dari serangan cyber, dan selalu gunakan setiap serangan cyber sebagai alat pendidikan untuk meningkatkan keseluruhan rencana keamanan Anda.

Terorisme dunia maya adalah raksasa 24/7, 365 hari setahun yang tidak pernah tidur; tidak perlu makan dan tidak pernah berhenti memangsa. Mengembangkan pendekatan berlapis-lapis untuk melawan raksasa ini akan meminimalkan eksploitasi kerentanan, memungkinkan orang, organisasi, dan negara untuk tidur lebih nyenyak di malam hari.

13.11 RINGKASAN

Terorisme dunia maya adalah topik yang sangat hangat di seluruh dunia dan negara-negara terlibat untuk mengembangkan mekanisme konkret untuk memeranginya dan pengaruhnya terhadap instrumen negara. Dalam unit ini konsep cyber terrorism dan pengertian umumnya, jenis-jenis cyber terrorism, pengaruh cyber terrorism di kancah nasional, infrastruktur internasional, karakteristik cyber terrorism, cyber terrorism-tantangan dan permasalahannya, siapa cyber terorisnya, serangan komputer dan cyber terorisme, tujuh jenis motivasi Hacker, dan strategi menghadapi ancaman cyber terrorism dibahas panjang lebar untuk memahami isu-isu terkait cyber terrorism.

13.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Authorpress)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang tepat dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

13.13 PERIKSA KEMAJUAN ANDA

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Beberapa contoh kegiatan terorisme dunia maya termasuk pengeboman email, peretasan ke situs web portal/perbankan/rumah sakit pemerintah, dll.
b) Terorisme siber adalah serangan terencana dan bermotif politik terhadap informasi, sistem komputer, program komputer, dan data.
c) Niat serangan terorisme siber dapat berkisar dari gangguan ekonomi melalui jaringan dan sistem keuangan.
d) Terorisme siber terkadang dibedakan dari perang siber, yaitu serangan berbasis komputer oleh agen-agen negara-bangsa.

e) Serangan fisik melibatkan senjata konvensional yang ditujukan terhadap fasilitas komputer atau jalur transmisinya.

B. Isi Bagian yang Kosong:

I. Sebuah bom e-mail dapat dianggap .....oleh beberapa orang dan terorisme dunia maya oleh orang lain.
II. .....virus menelan biaya hampir 10 miliar, sulit untuk memahami implikasi keuangan dari serangan yang jauh lebih serius dan komprehensif.
III. Seorang pemrogram yang.....
IV. Informasi sebagai bentuk terorisme siber.
V. ....., selama operasi Badai Gurun, militer AS dilaporkan mengganggu pusat komunikasi dan komputer Irak.
VI. Peretas Topi Putih adalah.....

13.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Hacktivisme
2. Serangga cinta
3. Mendobrak sistem komputer untuk mencuri atau mengubah atau menghancurkan
4. Pada tahun 1991
5. Orang Baik

13.15 PERTANYAAN TERMINAL

1. Apa pengertian dan jenis-jenis cyber terrorism?
2. Apa pengaruh terorisme siber terhadap infrastruktur nasional/internasional?
3. Apa saja ciri-ciri terorisme siber?
4. Siapa teroris dunia maya?
5. Apa saja tujuh jenis motivasi hacker?

BAB 14
TERORISME CYBER: PERSPEKTIF GLOBAL

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan terkait Cyber Terrorism dengan mengacu pada Perspektif Global
- Memahami pentingnya Putusan Peradilan yang disampaikan oleh berbagai badan
- Memahami masalah teknis dan hukum terkait Cyber Terrorism dengan mengacu pada Perspektif Global

14.1. PENGANTAR

Terorisme dunia maya adalah penggunaan kegiatan yang mengganggu atau ancamannya secara terencana, di ruang maya, dengan maksud untuk memajukan tujuan sosial, ideologis, agama, politik atau serupa, atau untuk mengintimidasi siapa pun dalam memajukan tujuan tersebut. Komputer dan internet menjadi bagian penting dari kehidupan kita sehari-hari. Mereka digunakan oleh individu dan masyarakat untuk membuat hidup mereka lebih mudah. Mereka menggunakannya untuk menyimpan informasi, memproses data, mengirim dan menerima pesan, komunikasi, mengendalikan mesin, mengetik, mengedit, mendesain, menggambar, dan hampir semua aspek kehidupan. Akibat paling mematikan dan destruktif dari ketidakberdayaan ini adalah munculnya konsep “cyber terrorism”. Konsep dan metode tradisional terorisme telah mengambil dimensi baru, yang sifatnya lebih destruktif dan mematikan. Di era teknologi informasi para teroris telah memperoleh keahlian untuk menghasilkan kombinasi senjata dan teknologi yang paling mematikan, yang jika tidak dijaga dengan baik pada waktunya, akan memakan korbannya sendiri.

Kerusakan yang dihasilkan akan hampir tidak dapat diubah dan paling bencana di alam. Singkatnya, kita menghadapi bentuk terorisme terburuk yang dikenal sebagai "Terorisme Cyber". Ungkapan "terorisme dunia maya" mencakup penggunaan negatif dan berbahaya yang disengaja dari teknologi informasi untuk menghasilkan efek yang merusak dan merugikan properti, baik berwujud maupun tidak berwujud, milik orang lain. Misalnya, meretas sistem komputer dan kemudian menghapus informasi bisnis yang berguna dan berharga dari pesaing saingan adalah bagian tak terpisahkan dari terorisme dunia maya. Definisi "terorisme dunia maya" tidak dapat dibuat lengkap karena sifat kejahatannya sedemikian rupa sehingga harus dibiarkan bersifat inklusif. Sifat "dunia maya" sedemikian rupa sehingga metode dan teknologi baru ditemukan secara teratur; maka tidak disarankan untuk menempatkan definisi dalam formula straightjacket atau merpati utuh. Padahal, upaya pertama yang harus dilakukan Pengadilan adalah menafsirkan definisi tersebut sebebas mungkin sehingga ancaman terorisme dunia maya dapat ditangani secara tegas dan dengan hukuman yang berat. Undang-undang yang menangani terorisme dunia maya, bagaimanapun, tidak cukup untuk memenuhi niat berbahaya para teroris dunia maya ini dan membutuhkan peremajaan dalam konteks dan perkembangan terbaru di seluruh dunia.

14.2 DEFINISI GLOBAL TERORISME CYBER

Meskipun ada beberapa definisi yang menjelaskan tentang istilah terorisme, salah satu definisi yang sering dijumpai adalah bahwa terorisme adalah "penggunaan yang melanggar hukum atau penggunaan paksaan atau kekerasan oleh seseorang atau kelompok terorganisir terhadap orang atau properti dengan maksud untuk mengintimidasi atau memaksa masyarakat atau pemerintah, seringkali untuk r_[mihm.' ideologis atau politik.' Interaksi antara motif manusia dan informasi Teknologi untuk kegiatan teroris di dunia maya atau di dunia maya dapat disebut sebagai cyber terrorism.Namun inilah definisi cyber terrorism yang digunakan Sarah Gordon dan Richard Ford dari Symantec dalam upaya mereka untuk mendefinisikan "Cyber terrorism murni" sebagai sebuah konsep memiliki berbagai definisi, sebagian besar karena setiap pakar keamanan memiliki definisinya sendiri. Istilah ini dapat didefinisikan sebagai penggunaan teknologi informasi oleh kelompok teroris atau individu untuk mencapai tujuan mereka.

Ini mungkin termasuk penggunaan teknologi informasi untuk mengatur dan melakukan serangan terhadap jaringan, sistem komputer dan infrastruktur telekomunikasi, dan untuk bertukar informasi dan p melakukan ancaman elektronik. Ancaman keamanan semacam ini dapat memanifestasikan dirinya dalam banyak cara, seperti meretas sistem komputer, memprogram virus dan worm, serangan halaman Web, melakukan serangan penolakan layanan (DoS), atau melakukan serangan teroris melalui komunikasi elektronik. Yang lebih umum adalah klaim bahwa terorisme dunia maya tidak ada dan sebenarnya itu adalah peretasan dan serangan jahat. Mereka yang mendukung klaim ini tidak setuju dengan istilah "terorisme" karena jika kita mempertimbangkan teknologi terkini untuk pencegahan dan perawatan, kemungkinan menciptakan ketakutan, kerusakan fisik yang signifikan, atau kematian di antara penduduk yang menggunakan sarana elektronik akan sangat kecil.

Pusat Perlindungan Infrastruktur Nasional AS mendefinisikan istilah tersebut sebagai, “Tindakan kriminal yang dilakukan dengan menggunakan komputer dan kemampuan telekomunikasi, yang mengakibatkan kekerasan dengan penggunaan komputer dan atau gangguan layanan untuk menciptakan ketakutan dengan menyebabkan kebingungan dan ketidakpastian dalam populasi tertentu, dengan tujuan mempengaruhi pemerintah atau populasi untuk sesuai dengan agenda politik, sosial atau ideologis tertentu." Center for Strategic and International Studies mendefinisikan Cyber Terrorism sebagai, "Penggunaan alat jaringan komputer untuk mematikan infrastruktur nasional yang kritis (seperti energi, transportasi, operasi pemerintah) atau untuk memaksa atau mengintimidasi pemerintah atau penduduk sipil". (Pusat Studi Infrastruktur Strategis (NIPS), sebelumnya merupakan unit Biro Investigasi federal (FBI) Ini melakukan penyelidikan dan memberikan tanggapan terhadap serangan komputer.)

Sebuah studi tahun 1999 yang disiapkan untuk Badan Intelijen Pertahanan dan diproduksi di Sekolah Pascasarjana Angkatan Laut dimulai dengan penafian yang menyatakan, "teror dunia maya bukanlah ancaman. Setidaknya belum, dan tidak untuk sementara waktu." Namun demikian, penulis memperingatkan, "teror dunia maya memang datang." Sekitar waktu yang sama, Richard Clarke, yang pada waktu itu adalah penasihat khusus Gedung Putih untuk keamanan dunia maya, lebih suka menggunakan istilah "perang info" daripada terorisme dunia maya. Lebih dari satu dekade kemudian, dia masih menolak kata terorisme

dunia maya atas dasar bahwa itu adalah ikan merah yang "menyihir gambar Bin Ladin mengobarkan perang dari guanya"; dia, bagaimanapun, memperingatkan bahwa mungkin ada istilah seperti terorisme cyber di masa depan. Barry Collin pertama kali memperkenalkan istilah terorisme dunia maya pada tahun 1980-an, meskipun para ahli belum membentuk konsensus definisi tentang terorisme, masih belum ada definisi yang menyatukan tentang terorisme dunia maya.

Terorisme dunia maya adalah istilah yang bahkan lebih buram daripada terorisme, menambahkan lapisan lain ke konsep yang sudah diperdebatkan. Peristiwa dunia maya pada umumnya sering disalahpahami oleh publik dan salah diberitakan oleh media. Orang-orang cenderung menggunakan istilah perang dunia maya, terorisme dunia maya, kejahatan dunia maya, dan peretasan secara bergantian, meskipun ada perbedaan penting, terkadang tidak kentara. Bruce Hoffman mendefinisikan terorisme sebagai "penciptaan dan eksploitasi rasa takut yang disengaja melalui kekerasan atau ancaman kekerasan dalam mengejar perubahan politik." Jika seseorang berasumsi sejenak bahwa ini adalah definisi terorisme yang diterima, maka penambahan dunia maya ke istilah ini menghasilkan definisi yang sederhana, meskipun melingkar: terorisme dunia maya adalah penggunaan dunia maya untuk melakukan terorisme.

Mengingat berbagai kegiatan terorisme dunia maya yang dijelaskan dalam literatur dan digambarkan dalam kelompok yang ditunjukkan pada Gambar 1 (lihat versi PDF), definisi sederhana ini dapat diperluas menjadi: terorisme dunia maya adalah penggunaan kemampuan dunia maya untuk melakukan tindakan yang memungkinkan, mengganggu, dan merusak. operasi militan di dunia maya untuk menciptakan dan mengeksploitasi ketakutan melalui kekerasan atau ancaman kekerasan dalam mengejar perubahan politik.

14.3 UPAYA HUKUM INTERNASIONAL

Sebelum diadopsinya resolusi 1373 (2001) dan pembentukan Komite Kontra-Terorisme, masyarakat internasional telah mengumumkan 12 dari 16 instrumen hukum internasional kontra-terorisme saat ini. Namun, tingkat kepatuhan terhadap konvensi dan protokol ini oleh Negara-negara Anggota Perserikatan Bangsa-Bangsa rendah. Sebagai hasil dari perhatian yang terfokus pada penanggulangan terorisme sejak peristiwa 11 September 2001 dan adopsi resolusi Dewan Keamanan 1373 (2001), yang menyerukan kepada Negara-negara untuk menjadi pihak dalam instrumen internasional ini, tingkat kepatuhan telah meningkat: sekitar dua -pertiga dari Negara Anggota PBB telah meratifikasi atau mengaksesi setidaknya 10 dari 16 instrumen, dan tidak ada lagi negara yang tidak menandatangani atau menjadi pihak setidaknya salah satu dari mereka. Antara tahun 1963 dan 2004, di bawah naungan Perserikatan Bangsa-Bangsa dan badan-badan khususnya, masyarakat internasional mengembangkan 13 instrumen kontraterorisme internasional yang terbuka untuk partisipasi semua Negara Anggota. Pada tahun 2005, masyarakat internasional juga memperkenalkan perubahan substantif pada tiga instrumen universal ini untuk secara khusus menjelaskan ancaman terorisme; pada tanggal 8 Juli tahun itu Negara-negara mengadopsi Amandemen terhadap Konvensi tentang Perlindungan Fisik Bahan Nuklir, dan pada tanggal 14 Oktober mereka menyetujui baik Protokol 2005 hingga Konvensi untuk Penindasan Tindakan Melanggar Hukum terhadap Keselamatan Navigasi Maritim dan Protokol tahun 2005 tentang

Protokol untuk Pemberantasan Tindakan Melanggar Hukum terhadap Keamanan Anjungan Tetap yang Berada di Landas Kontinen.

Majelis Umum telah memfokuskan pada terorisme sebagai masalah internasional sejak tahun 1972 dan, melalui tahun 1980-an, membahas masalah ini secara berkala melalui resolusi. Selama periode ini, Majelis juga mengadopsi dua instrumen yang berkaitan dengan kontra-terorisme: Konvensi tentang Pencegahan dan Penghukuman Kejahatan terhadap Orang yang Dilindungi Secara Internasional, termasuk Agen Diplomatik (tahun 1973) dan Konvensi Internasional Menentang Penyanderaan (tahun 1979).

Pada bulan Desember 1994, Majelis kembali mengarahkan perhatian pada masalah ini melalui Deklarasi tentang Tindakan untuk Menghapuskan Terorisme Internasional (A/RES/49/60). Pada tahun 1996, suplemen dari Deklarasi ini (A/RES/51/210) membentuk Komite Ad Hoc untuk mengelaborasi konvensi internasional untuk pemberantasan pemboman teroris dan, selanjutnya, sebuah konvensi internasional untuk penindasan tindakan terorisme nuklir, untuk melengkapi instrumen-instrumen internasional terkait yang ada, dan setelah itu membahas cara-cara untuk mengembangkan lebih lanjut suatu hukum yang komprehensif kerangka konvensi yang menangani terorisme internasional. Mandat ini terus diperbarui dan direvisi setiap tahun oleh Majelis Umum dalam resolusinya tentang topik tindakan untuk menghapus terorisme internasional.

Selama dekade terakhir, Negara-negara Anggota menyelesaikan tiga instrumen kontraterorisme lagi yang mencakup jenis kegiatan teroris tertentu: Konvensi Internasional 1997 untuk Penindasan Pengeboman Teroris; Konvensi Internasional 1999 untuk Pemberantasan Pendanaan Terorisme dan Konvensi Internasional untuk Pemberantasan Tindakan Terorisme Nuklir. Yang terakhir diadopsi pada April 2005 dan dibuka untuk ditandatangani pada 14 September 2005, hari pertama KTT Dunia Majelis Umum. Selama pertemuan tingkat tinggi tiga hari itu, ditandatangani oleh 82 Negara Anggota.

Juga dalam kerangka Komite Ad Hoc bahwa Negara-negara Anggota telah merundingkan rancangan konvensi komprehensif tentang terorisme internasional sejak tahun 2000.

14.4 PEMBERANTASAN PENDANAAN TERORISME

Resolusi 1373 (2001) Juga Membentuk Komite untuk Memantau Implementasi: Menegaskan kembali kecamannya yang tegas atas tindakan teroris yang terjadi di New York, Washington, D.C., dan Pennsylvania pada 11 September, Dewan Keamanan malam ini dengan suara bulat mengadopsi resolusi yang luas dan komprehensif. resolusi dengan langkah dan strategi memerangi terorisme internasional. Dengan resolusi 1373 (2001) Dewan juga membentuk Komite Dewan untuk memantau pelaksanaan resolusi dan memanggil semua Negara untuk melaporkan tindakan yang telah mereka lakukan untuk tujuan itu selambat-lambatnya 90 hari dari hari ini. Berdasarkan ketentuan teks Dewan memutuskan bahwa semua Negara harus mencegah dan menekan pendanaan terorisme, serta mengkriminalisasi penyediaan atau pengumpulan dana yang disengaja untuk tindakan tersebut.

Dana, aset keuangan dan sumber daya ekonomi dari mereka yang melakukan atau mencoba melakukan tindakan teroris atau berpartisipasi dalam atau memfasilitasi pelaksanaan tindakan teroris dan orang-orang dan entitas yang bertindak atas nama teroris

juga harus dibekukan tanpa penundaan. Dewan juga memutuskan bahwa Negara harus melarang warga negara mereka atau orang atau entitas di wilayah mereka dari menyediakan dana, aset keuangan, sumber daya ekonomi, keuangan atau layanan terkait lainnya yang tersedia untuk orang yang melakukan atau mencoba untuk melakukan, memfasilitasi atau berpartisipasi dalam tindakan teroris. tindakan. Negara juga harus menahan diri dari memberikan segala bentuk dukungan kepada entitas atau orang yang terlibat dalam aksi teroris; mengambil langkah-langkah yang diperlukan untuk mencegah dilakukannya tindakan teroris; menyangkal tempat berlindung yang aman bagi mereka yang membiayai, merencanakan, mendukung, melakukan tindakan teroris dan juga menyediakan tempat berlindung yang aman.

Dengan ketentuan lain, Dewan memutuskan bahwa semua Negara harus mencegah mereka yang membiayai, merencanakan, memfasilitasi atau melakukan tindakan teroris menggunakan wilayah mereka masing-masing untuk tujuan tersebut terhadap negara lain dan warganya. Negara juga harus memastikan bahwa siapa pun yang telah berpartisipasi dalam pendanaan, perencanaan, persiapan atau perbuatan teroris atau dalam mendukung tindakan teroris dibawa ke pengadilan. Mereka juga harus memastikan bahwa tindakan teroris ditetapkan sebagai tindak pidana serius dalam undang-undang dan peraturan domestik dan bahwa keseriusan tindakan tersebut sepatutnya tercermin dalam hukuman yang dijatuhkan. Juga melalui teks, Dewan meminta semua Negara untuk mengintensifkan dan mempercepat pertukaran informasi mengenai tindakan atau gerakan teroris; dokumen palsu atau palsu; lalu lintas senjata dan bahan sensitif; penggunaan komunikasi dan teknologi oleh kelompok teroris; dan ancaman yang ditimbulkan oleh kepemilikan senjata pemusnah massal.

Negara-negara juga diminta untuk bertukar informasi dan bekerja sama untuk mencegah dan menekan tindakan teroris dan untuk mengambil tindakan terhadap para pelaku tindakan tersebut. Negara-negara harus menjadi pihak, dan menerapkan sepenuhnya sesegera mungkin, konvensi dan protokol internasional yang relevan untuk memerangi terorisme. Berdasarkan teks tersebut, sebelum memberikan status pengungsi, semua Negara harus mengambil langkah-langkah yang tepat untuk memastikan bahwa para pencari suaka tidak merencanakan, memfasilitasi atau berpartisipasi dalam aksi teroris. Selanjutnya, Negara harus memastikan bahwa status pengungsi tidak disalahgunakan oleh pelaku, penyelenggara atau fasilitator aksi teroris, dan bahwa klaim motivasi politik tidak diakui sebagai alasan untuk menolak permintaan ekstradisi terhadap terduga teroris.

Dewan mencatat dengan prihatin hubungan erat antara terorisme internasional dan kejahatan terorganisir transnasional, obat-obatan terlarang, pencucian uang dan pergerakan ilegal bahan nuklir, kimia, biologi dan bahan mematikan lainnya. Sehubungan dengan itu, ditekankan perlunya meningkatkan koordinasi upaya nasional, sub regional, regional dan internasional untuk memperkuat respons global terhadap ancaman keamanan internasional tersebut. Menegaskan kembali kebutuhan untuk memerangi dengan segala cara, sesuai dengan Piagam, ancaman terhadap perdamaian dan keamanan internasional yang disebabkan oleh tindakan teroris, Dewan menyatakan tekadnya untuk mengambil semua langkah yang diperlukan untuk sepenuhnya melaksanakan resolusi saat ini.

14.5 AKSI PBB UNTUK MELAWAN TERORISME

Dipandu oleh resolusi Dewan Keamanan 1373 (2001) dan 1624 (2005), CTC bekerja untuk meningkatkan kemampuan Negara-negara Anggota Perserikatan Bangsa-Bangsa untuk mencegah tindakan teroris baik di dalam perbatasan mereka maupun lintas wilayah. Itu didirikan setelah serangan teroris 11 September di Amerika Serikat. Raimonda Murmokaitė, Duta Besar dan Perwakilan Tetap Lithuania, menjabat sebagai ketua Komite pada Januari 2014.

CTC dibantu oleh Counter-Terrorism Committee Executive Directorate (CTED), yang melaksanakan keputusan kebijakan Komite, melakukan penilaian ahli dari setiap Negara Anggota dan memfasilitasi bantuan teknis kontra-terorisme ke negara-negara. Resolusi 1373 (2001), diadopsi dengan suara bulat pada tanggal 28 September 2001, menyerukan kepada Negara-negara Anggota untuk menerapkan sejumlah tindakan yang dimaksudkan untuk meningkatkan kemampuan hukum dan kelembagaan mereka untuk melawan kegiatan teroris, termasuk mengambil langkah-langkah untuk:

- Kriminalisasi pendanaan terorisme
- Membekukan tanpa penundaan dana apapun yang terkait dengan orang-orang yang terlibat dalam aksi terorisme
- Tolak semua bentuk dukungan keuangan untuk kelompok teroris
- Menekan penyediaan tempat berlindung yang aman, rezeki atau dukungan untuk teroris
- Berbagi informasi dengan pemerintah lain tentang kelompok mana pun yang mempraktikkan atau merencanakan aksi teroris
- Bekerja sama dengan pemerintah lain dalam penyelidikan, deteksi, penangkapan, ekstradisi dan penuntutan mereka yang terlibat dalam tindakan tersebut; dan
- Mengkriminalisasi bantuan aktif dan pasif untuk terorisme dalam hukum domestik dan membawa pelanggarnya ke pengadilan.

Resolusi tersebut juga menyerukan kepada Negara-negara untuk menjadi pihak, sesegera mungkin, pada instrumen hukum kontra-terorisme internasional yang relevan.

Resolusi 1624 (2005) berkaitan dengan hasutan untuk melakukan tindakan terorisme, menyerukan kepada Negara-negara Anggota PBB untuk melarangnya oleh hukum, mencegah tindakan tersebut dan menolak tempat berlindung yang aman bagi siapa pun "dengan hormat kepada siapa ada informasi yang kredibel dan relevan yang memberikan alasan serius untuk mempertimbangkan bahwa mereka telah bersalah atas perilaku seperti itu." Metode Kerja: Singkatnya, pekerjaan CTC dan CTED terdiri dari:

- Kunjungan negara - atas permintaan mereka, untuk memantau kemajuan, serta untuk mengevaluasi sifat dan tingkat bantuan teknis yang mungkin diperlukan suatu negara untuk mengimplementasikan resolusi 1373 (2001);
- Bantuan teknis - untuk membantu menghubungkan negara-negara dengan program bantuan teknis, keuangan, peraturan dan legislatif yang tersedia, serta donor potensial;
- Laporan negara – untuk memberikan gambaran menyeluruh tentang situasi kontra-terorisme di setiap negara dan berfungsi sebagai alat untuk dialog antara Komite dan Negara Anggota;

- Praktik terbaik – untuk mendorong negara menerapkan praktik, kode, dan standar terbaik yang diketahui, dengan mempertimbangkan keadaan dan kebutuhan mereka sendiri; dan
- Pertemuan khusus – untuk mengembangkan hubungan yang lebih erat dengan organisasi internasional, regional dan sub regional yang relevan, dan untuk membantu menghindari duplikasi usaha dan pemborosan sumber daya melalui koordinasi yang lebih baik

Komite Kontra-Terorisme (CTC) dibentuk oleh resolusi Dewan Keamanan 1373 (2001), yang diadopsi dengan suara bulat pada 28 September 2001 setelah serangan teroris 11 September di Amerika Serikat. Komite, yang terdiri dari 15 anggota Dewan Keamanan, ditugaskan untuk memantau pelaksanaan resolusi 1373 (2001), yang meminta negara-negara untuk menerapkan sejumlah langkah yang dimaksudkan untuk meningkatkan kemampuan hukum dan kelembagaan mereka untuk melawan kegiatan teroris di dalam negeri, di wilayah mereka dan di seluruh dunia, termasuk mengambil langkah-langkah untuk:

- Kriminalisasi pendanaan terorisme
- Membekukan tanpa penundaan dana apapun yang terkait dengan orang-orang yang terlibat dalam aksi terorisme
- Tolak semua bentuk dukungan keuangan untuk kelompok teroris
- Menekan penyediaan tempat berlindung yang aman, rezeki atau dukungan untuk teroris
- Berbagi informasi dengan pemerintah lain tentang kelompok mana pun yang mempraktikkan atau merencanakan aksi teroris
- Bekerja sama dengan pemerintah lain dalam penyelidikan, deteksi, penangkapan, ekstradisi dan penuntutan mereka yang terlibat dalam tindakan tersebut; dan
- Mengkriminalisasi bantuan aktif dan pasif untuk terorisme dalam hukum domestik dan membawa pelanggarnya ke pengadilan.

Resolusi tersebut juga menyerukan kepada Negara-negara untuk menjadi pihak, sesegera mungkin, pada instrumen hukum kontra-terorisme internasional yang relevan. Pada bulan September 2005, Dewan Keamanan mengadopsi resolusi 1624 (2005) tentang hasutan untuk melakukan tindakan terorisme, menyerukan kepada Negara-negara Anggota PBB untuk melarangnya berdasarkan hukum, mencegah tindakan tersebut dan menolak tempat berlindung yang aman bagi siapa pun "yang dapat dipercaya dan informasi yang relevan memberikan alasan serius untuk mempertimbangkan bahwa mereka telah bersalah atas perilaku tersebut." Resolusi itu juga meminta negara-negara untuk melanjutkan upaya internasional untuk meningkatkan dialog dan memperluas pemahaman di antara peradaban. Dewan Keamanan mengarahkan CTC untuk memasukkan resolusi 1624 (2001) dalam dialog yang sedang berlangsung dengan negara-negara tentang upaya mereka untuk melawan terorisme.

Direktorat Eksekutif Komite Kontra-Terorisme (CTED)

Berdasarkan resolusi 1535 (2004), Dewan Keamanan membentuk Direktorat Eksekutif Komite Kontra-Terorisme (CTED) untuk membantu pekerjaan CTC dan mengkoordinasikan proses pemantauan pelaksanaan resolusi 1373 (2001). CTED menjadi staf penuh pada September 2005 dan secara resmi dinyatakan beroperasi pada Desember 2005. Mandat CTED

diperpanjang hingga akhir 2013 dengan resolusi Dewan Keamanan S/RES/1963 (2010). CTED terdiri dari sekitar 40 anggota staf, sekitar setengahnya adalah ahli hukum yang menganalisis laporan yang disampaikan oleh Negara-negara di bidang-bidang seperti penyusunan undang-undang, pendanaan terorisme, kontrol perbatasan dan bea cukai, polisi dan penegakan hukum, hukum pengungsi dan migrasi, perdagangan senjata. dan keamanan maritim dan transportasi. CTED juga memiliki pejabat senior hak asasi manusia. CTED dibagi menjadi dua bagian: Assessment and Technical Assistance Office (ATAO), yang selanjutnya dibagi menjadi tiga kelompok geografis untuk memungkinkan para ahli mengkhususkan diri di wilayah tertentu di dunia, dan Administrasi dan Kantor Informasi (AIO).

Selain itu, lima kelompok teknis bekerja secara horizontal di seluruh ATAO untuk mengidentifikasi masalah dan kriteria untuk membuat penilaian di bidang keahlian teknis khusus mereka dan kemudian menyebarluaskannya ke tiga klaster. Masing-masing kelompok menangani bantuan teknis; pendanaan teroris; kontrol perbatasan, perdagangan senjata dan penegakan hukum; masalah hukum umum, termasuk legislasi, ekstradisi, dan bantuan hukum timbal balik; dan terakhir, isu-isu yang diangkat oleh resolusi 1624 (2005); serta aspek HAM kontra-terorisme dalam konteks resolusi 1373 (2001). Di seluruh AIO, ada juga unit kendali mutu untuk meningkatkan kualitas teknis dan konsistensi dalam bahasa dan format dokumen CTED dan unit komunikasi dan penjangkauan publik untuk memperkuat kegiatan penjangkauannya. Untuk mendukung pekerjaan Komite pada resolusi 1624 (2005), CTED telah menyiapkan dua laporan (S/2006/737 dan S/2008/2) yang merangkum tanggapan yang diajukan sejauh ini oleh sekitar setengah dari keanggotaan PBB.

14.6 TERORISME CYBER YAITU KEJAHATAN CYBER

"Terorisme dunia maya juga jelas merupakan ancaman yang muncul. Kelompok teroris semakin paham komputer, dan dan beberapa mungkin memperoleh kemampuan untuk menggunakan serangan dunia maya untuk menimbulkan gangguan yang terisolasi dan singkat terhadap infrastruktur AS. Karena prevalensi alat peretas yang tersedia untuk umum, banyak dari kelompok-kelompok ini mungkin sudah memiliki kemampuan untuk meluncurkan penolakan layanan dan serangan gangguan lainnya terhadap sistem yang terhubung ke Internet. Ketika teroris menjadi lebih paham komputer, opsi serangan mereka hanya akan meningkat." (War on Terrorism, 2003) Inilah yang Robert Mueller, Direktur FBI, bersaksi pada 11 Februari 2003 di hadapan Senat AS dalam dengar pendapat tentang War On Terrorism melawan Al-Qaeda dan organisasi teroris lainnya.

AS dan organisasi media global mengambil kesaksian ini dan mulai berspekulasi tentang kemungkinan serangan teroris Cyber skala besar. Sejauh ini, serangan seperti itu belum terwujud. Pada saat yang sama istilah yang sama, Cybercrime, digunakan untuk menggambarkan kegiatan kriminal di Internet seperti pencurian identitas, pelanggaran hak cipta dan penipuan bank, tetapi sering kali kedua istilah ini (Cybercrime dan Cyber terrorism) akhirnya digunakan secara bergantian dan maknanya, terutama bagi publik, menjadi kabur dan tidak jelas. Pemerintah, jaringan kebijakan dan media di seluruh dunia telah terlibat dalam upaya membangun pertahanan terhadap serangan Cyber, memberlakukan peraturan baru sambil mempertahankan suasana yang hampir mitologis atas ancaman dan risiko potensi Cybercrime dan serangan teroris Cyber.

Karena jangkauan global Internet terus berkembang, pengaruhnya pada semua bidang usaha manusia online menjadi lebih luas. Individu atau kelompok dapat mengeksploitasi anonimitas yang diberikan oleh dunia maya untuk terlibat dalam kegiatan ilegal atau terlarang yang bertujuan untuk mengintimidasi, membahayakan, mengancam, atau menimbulkan ketakutan bagi warga, komunitas, organisasi, atau negara. Jarak virtual dan fisik antara penyerang dan korban dan kesulitan dalam melacak kembali serangan ke individu meminimalkan ancaman penangkapan yang melekat pada penyerang. Tetapi bagaimana aktivitas tersebut didefinisikan? Apa itu Cybercrime dan apa ciri-cirinya? Bagaimana seorang Cyberterrorist dapat diidentifikasi dan apa perbedaannya dari Cybercriminal? Sejauh ini, definisi Cybercrime dan Cyber terrorism dalam literatur, dokumen pemerintah, dan penggunaan sehari-hari sangat bervariasi, spesifik konteks dan sarat emosional, yang membuat wacana tentang subjek menjadi sulit. FBI sendiri telah menerbitkan tiga definisi berbeda tentang terorisme Cyber: "Terorisme yang memulai ... serangan terhadap informasi" pada tahun 1999, hingga "penggunaan alat Cyber" pada tahun 2000 dan "tindakan kriminal yang dilakukan dengan penggunaan komputer" pada tahun 2004 (Baranetsky, 2009). Cybercrime dan Cyber terrorism telah digunakan untuk menggambarkan tindakan online seperti:

- Peretasan / Cracking topi hitam
- Pelanggaran seks anak (pornografi dan dandanan)
- Kejahatan di dunia maya
- Aktivisme dunia maya / Hacktivisme
- Penulisan virus dan malware
- Penguntit dunia maya
- Pencurian identitas / Penipuan
- Transaksi keuangan ilegal / Pencucian uang
- Pelanggaran hak cipta
- Tindakan cyber bullying yang serius
- Serangan penolakan layanan
- Rogue bot-net

Cyber terrorism biasanya memiliki arti yang lebih kuat daripada Cybercrime, menggambarkan tindakan yang memiliki karakteristik serupa dengan serangan terorisme dunia nyata, tetapi tidak selalu. Di sisi lain, Cybercrime sering digunakan sebagai istilah umum untuk menggambarkan aktivitas ilegal, berbahaya dan/atau bermusuhan di Internet (termasuk terorisme Cyber). Selain itu, istilah lain terkadang digunakan untuk menggambarkan tindakan online terlarang yang serupa, yang semakin memperumit masalah, dan penggunaannya biasanya bergantung pada konteks atau orang/organisasi yang menggunakannya. Misalnya, seorang juru bicara dalam militer kemungkinan akan menggunakan istilah Perang siber untuk menggambarkan tindakan daring yang bermusuhan antara dua negara dan/atau tindakan terorisme yang berasal dari negara lain dan dimanifestasikan secara daring (bukan menggunakan istilah Terorisme dunia maya).

Sebelum mencoba mendefinisikan terorisme Cyber dan Cybercrime, kita harus merenungkan validitas kedua istilah tersebut. Taipale (2010) berpendapat bahwa "Terorisme siber, apa pun itu, adalah istilah yang tidak berguna" dan dia percaya bahwa, "teroris akan

menggunakan alat strategis apa pun yang mereka bisa" sehingga terorisme Cyber tidak lebih penting daripada bentuk lainnya. Argumen serupa dapat dibuat untuk Cybercrime, seperti Wall (2008) mengatakan, "Cybercrime relatif tidak berarti dengan sendirinya karena merupakan konstruksi fiksi yang tidak memiliki titik acuan asli dalam hukum, ilmu pengetahuan atau tindakan sosial." Namun, istilah ini secara bertahap mendapatkan landasan dalam wacana hukum formal karena undang-undang baru di banyak negara seperti Australia (Cybercrime Act 2001), Nigeria (Draft Cybercrime Act), Amerika Serikat (Usulan Cybercrime Act 2007) dan Inggris (The Home Office memperkenalkan Strategi Kejahatan Dunia Maya pada Maret 2010).

Lapisan kerumitan tambahan ditambahkan ketika kita melihat sistem hukum dari berbagai negara dan definisi mereka yang beragam tentang tindakan melanggar hukum. Bukan hal yang aneh jika satu negara mendefinisikan sebagai tindak pidana hanya menjadi kesalahan perdata di negara lain. Masalah muncul ketika seseorang adalah penerima berita tentang serangan teroris Cyber di negara asing, yang hanya akan dicirikan sebagai upaya peretasan atau protes aktivisme Cyber di negaranya sendiri, dan sebaliknya. Dengan demikian, kemungkinan besar seseorang dapat menunjukkan perasaan takut, tidak aman, cemas, atau panik yang tidak beralasan, bersama dengan kebingungan umum tentang cara menafsirkan berita.

Kejahatan dunia maya dan terorisme dunia maya adalah dua masalah yang kemungkinan akan terus ada selama bertahun-tahun yang akan datang dan pasti harus ditangani. Tetapi proses ini perlu dilakukan dengan cara yang akan memastikan pertumbuhan Internet secara inklusif dan terbuka, mempertahankan prinsip-prinsip dasar yang telah dibangun di atasnya. Salah satu isu utama adalah disambiguasi dari istilah Cybercrime dan Cyber terrorism. Badan-badan pemerintah, jaringan kebijakan, cendekiawan, media, dan orang-orang perlu terlibat dalam percakapan global yang akan membantu mengungkap kejahatan dunia maya dan menentukan apa yang dimaksud dengan kejahatan dunia maya dan bagaimana penjahat dunia maya harus ditangani.

Terorisme dunia maya harus dipisahkan dari kejahatan dunia maya dan ditentukan secara realistis, seperti apa kemungkinan ancaman dari tindakan teroris dunia maya dan sejauh mana masyarakat harus menghadapi efek tersebut. Setelah kedua istilah ini didefinisikan dengan jelas dan tidak ambigu, orang akan jauh lebih siap untuk menerima dan memahami berita dan kebijakan terkait, dan akan dapat terlibat dalam wacana yang bermakna tentang subjek tersebut. Ini akan membantu mengurangi ketakutan yang tidak beralasan sementara pada saat yang sama memungkinkan individu untuk membuat keputusan yang tepat ketika mempertimbangkan kebijakan baru yang diusulkan dengan menimbang pro versus kontra dan dampaknya pada berbagai tingkat, jangka panjang dan pendek, alih-alih menyerah pada rasa takut dan kehilangan privasi dan kebebasan online mereka untuk keamanan yang lebih baik.

Peran media (televisi, blog, outlet berita online, dan lainnya) sangat penting dalam proses mendidik publik dan terlibat dalam percakapan, karena mereka akan menjadi mediator dan kurator informasi dan wacana tentang masalah tersebut. Dengan demikian, pendekatan yang ringkas dan masuk akal, tanpa praktik ketakutan dan kejutan, harus diikuti. Karena ini adalah masalah internasional, pemerintah dan jaringan kebijakan di seluruh dunia harus

berkumpul dan berdiskusi secara terbuka tentang apa yang lebih baik bagi warganya. Cendekiawan dan akademisi dapat memberikan keahlian yang berharga tentang masalah teknologi, psikologis, etika, dan lainnya, sambil menyoroti keraguan apa pun oleh mereka yang terlibat dalam proses tersebut.

Orang-orang di komunitas lokal, keluarga, dan jejaring sosial mereka harus saling membantu dan melatih untuk meningkatkan tingkat literasi internet rekan-rekan mereka dan menyoroti keunggulan web. Tingkat literasi Internet yang lebih tinggi dapat membantu orang melindungi diri mereka sendiri lebih baik dengan mengambil langkah-langkah keamanan sederhana, seperti menggunakan perangkat lunak anti-virus dan mengidentifikasi potensi risiko atau penipuan dalam transaksi keuangan online mereka.

14.7 PERANG CYBER DAN TERORISME CYBER

Istilah seperti "perang dunia maya" dan "terorisme dunia maya" telah banyak digunakan di media, dalam laporan resmi pemerintah dan di kalangan akademisi. Bahkan jika mereka sering dihipnotis, para ahli sepakat bahwa kecil kemungkinan perang cyber akan terjadi di masa depan (Thomas Rid dan Bruce Scheneier; sebaliknya, Jeffrey Carr). Meskipun demikian, mereka mengakui bahwa ancaman dunia maya adalah nyata dan bahwa berbagai alat dan teknik dunia maya menjadi semakin penting dalam konflik internasional, termasuk yang digunakan untuk sabotase, spionase, dan subversi. Elemen umum di antara keduanya adalah kurangnya definisi yang diterima secara internasional.

Pakar keamanan pemerintah AS Richard A. Clarke, dalam bukunya Cyber War, mendefinisikan "perang dunia maya" sebagai "tindakan oleh negara-bangsa untuk menembus komputer atau jaringan negara lain dengan tujuan menyebabkan kerusakan atau gangguan". Kurangnya pemahaman bersama membuka berbagai masalah lain:

- Bagaimana mungkin merumuskan definisi "perang dunia maya" sementara menghadapi ketidakmungkinan membuktikan sumber serangan?
- Mana yang mungkin berimplikasi pada hak membela diri dan aturan keterlibatan?
- Tanpa atribusi yang jelas, bagaimana mungkin membedakan tindakan perang siber dari serangan terorisme siber?

Kata "terorisme dunia maya" mengacu pada dua elemen: dunia maya dan terorisme. Mark Pollitt membangun definisi kerja seperti berikut:

“Terorisme siber adalah serangan yang direncanakan dan bermotivasi politik terhadap informasi, sistem komputer, program komputer, dan data yang mengakibatkan kekerasan terhadap sasaran non-kombatan oleh kelompok sub-nasional atau agen rahasia.” Definisi ini tentu sempit. Agar istilah "terorisme dunia maya" memiliki arti apa pun, kita harus dapat membedakannya dari jenis penyalahgunaan komputer lainnya seperti kejahatan komputer, spionase ekonomi, atau perang informasi. Saya akan menyarankan bahwa yang terakhir adalah fungsi ofensif dan defensif pemerintah. Pertama-tama penting untuk dicatat bahwa tidak ada definisi tunggal jika "terorisme" telah diterima secara universal. Selain itu, tidak ada definisi tunggal untuk istilah "terorisme dunia maya" yang diterima secara universal. Juga, pelabelan serangan komputer sebagai "terorisme dunia maya" bermasalah, karena seringkali sulit untuk menentukan niat, identitas, atau motivasi politik penyerang komputer dengan pasti sampai lama setelah peristiwa itu terjadi.

Kode Stuxnet, spionase dunia maya yang diduga berasal dari China, dan serangan ke Estonia dan Georgia telah dilaporkan secara luas sebagai contoh terorisme dunia maya dan kemungkinan tindakan perang dunia maya . Investigasi mendalam atas insiden-insiden tersebut tidak dapat membuktikan kepengarangan negara berdaulat maupun kerugian serius sebagai akibat dari serangan tersebut. Ini adalah salah satu masalah yang paling mendasar: Dalam relatif anonimitas dan kompleksitas Internet dan kemampuan untuk melintasi perbatasan internasional dan yurisdiksi dengan impunitas, sangat sulit untuk mengetahui dengan tepat siapa yang berada di balik serangan dan motif mereka yang sebenarnya.

14.8 STUDI KASUS INTERNASIONAL-I

Menganalisis Serangan Cyber di bawah Jus ad Bellum- Hukum perang dibagi menjadi dua bidang utama, jus ad bellum dan jus in bello. Jus ad bellum, juga dikenal sebagai hukum manajemen konflik, adalah rezim hukum yang mengatur transisi dari damai ke perang. Ini pada dasarnya menjabarkan kapan negara dapat secara sah menggunakan konflik bersenjata. Jus in bello, juga dikenal sebagai hukum konflik bersenjata, mengatur penggunaan kekuatan yang sebenarnya selama perang. Analisis apakah negara dapat merespons serangan cyber dengan pertahanan aktif sebagian besar berada di bawah jus ad bellum, karena jus ad bellum menetapkan ambang batas yang harus dilewati serangan cyber untuk dianggap sebagai tindakan perang.

Secara historis, transisi dari perdamaian ke perang berada di bawah hak prerogatif penguasa; namun, ia berada di bawah hukum internasional setelah Perang Dunia II dengan ratifikasi Piagam PBB. Meskipun Piagam PBB bukan satu-satunya sumber jus ad bellum, namun merupakan titik awal untuk semua analisis jus ad bellum. Pasal-pasal yang relevan dari Piagam PBB adalah Pasal 2(4), 39, dan 51, yang memberikan kerangka bagi analisis jus ad bellum modern.

Serangan cyber merupakan teka-teki bagi sarjana hukum. Serangan dunia maya datang dalam berbagai bentuk, potensi destruktifnya hanya dibatasi oleh kreativitas dan keterampilan penyerang di belakangnya. Meskipun tampaknya intuitif bahwa serangan dunia maya dapat merupakan serangan bersenjata, terutama mengingat kemampuannya untuk melukai atau membunuh, komunitas hukum enggan mengadopsi pendekatan ini karena serangan dunia maya tidak menyerupai serangan bersenjata tradisional dengan senjata konvensional. Lebih lanjut mengaburkan perairan hukum adalah pandangan yang salah dari negara dan cendekiawan sama-sama tentang perlunya negara untuk menghubungkan serangan dunia maya ke negara atau agennya sebelum merespons dengan kekuatan.

Meskipun benar bahwa serangan dunia maya tidak menyerupai serangan bersenjata tradisional, dan bahwa serangan dunia maya sulit untuk dikaitkan, tidak satu pun dari karakteristik ini yang dapat menghalangi negara untuk merespons dengan kekuatan. Bagian ini mengeksplorasi model analitis yang berbeda untuk menilai serangan bersenjata, makna logis dari tugas pencegahan yang berkaitan dengan serangan dunia maya, dan kapasitas teknologi program pelacakan untuk melacak serangan kembali ke titik asalnya. Setelah semua masalah ini diperiksa, menjadi jelas bahwa negara dapat secara legal menggunakan pertahanan aktif terhadap serangan dunia maya yang berasal dari negara yang melanggar kewajibannya untuk mencegahnya.

Serangan Cyber sebagai Serangan Bersenjata

Negara korban harus dapat mengklasifikasikan serangan siber sebagai serangan bersenjata atau serangan bersenjata yang akan segera terjadi sebelum merespons dengan pertahanan aktif karena, seperti yang telah kita diskusikan sebelumnya dalam bab ini, serangan bersenjata dan serangan bersenjata yang akan segera terjadi adalah pemicu yang memungkinkan negara untuk merespons secara mandiri. -pertahanan atau pertahanan diri antisipatif.

Idealnya, akan ada aturan yang jelas untuk mengklasifikasikan serangan dunia maya sebagai serangan bersenjata, serangan bersenjata yang akan segera terjadi, atau penggunaan kekuatan yang lebih rendah. Sayangnya, karena serangan dunia maya adalah bentuk serangan yang relatif baru, upaya internasional untuk mengklasifikasikannya masih dalam tahap awal, meskipun prinsip-prinsip hukum inti yang mengatur serangan bersenjata telah ditetapkan dengan baik. Akibatnya, apakah serangan siber dapat dikualifikasikan sebagai serangan bersenjata dan serangan siber mana yang harus dianggap sebagai serangan bersenjata masih menjadi pertanyaan terbuka dalam hukum internasional. Untuk menjawab pertanyaan-pertanyaan ini, subbagian ini mengkaji prinsip-prinsip hukum inti yang mengatur serangan bersenjata, menerapkannya pada serangan dunia maya, menjelaskan mengapa serangan dunia maya dapat dikualifikasikan sebagai serangan bersenjata, dan upaya untuk memberikan beberapa wawasan tentang serangan dunia maya mana yang harus dianggap sebagai serangan bersenjata.

"Serangan bersenjata" tidak didefinisikan oleh konvensi internasional mana pun. Akibatnya, maknanya dibiarkan terbuka untuk interpretasi oleh negara dan ulama. Meskipun ini mungkin terdengar bermasalah, sebenarnya tidak. Kerangka kerja untuk menganalisis serangan bersenjata relatif sudah mapan, seperti prinsip-prinsip hukum inti yang mengatur maknanya. Masyarakat internasional umumnya menerima uji ruang lingkup, durasi, dan intensitas Jean S. Pictet sebagai titik awal untuk mengevaluasi apakah penggunaan kekuatan tertentu merupakan dan serangan bersenjata. Di bawah uji Pictet, penggunaan kekuatan adalah serangan bersenjata jika cakupan, durasi, dan intensitasnya cukup. Tentu saja, seperti halnya dengan banyak konsep hukum internasional, negara, organisasi non-pemerintah, dan para sarjana semua menafsirkan ruang lingkup, durasi, dan uji intensitas secara berbeda.

Deklarasi negara membantu menyempurnakan penggunaan kekuatan mana yang memiliki cakupan, durasi, dan intensitas yang cukup untuk membentuk serangan bersenjata. Mengingat kembali Piagam PBB versi bahasa Prancis, yang mengacu pada "agresi bersenjata" daripada "serangan bersenjata", Jenderal PBB. Majelis meloloskan resolusi Definisi Agresi pada tahun 1974. Resolusi tersebut mensyaratkan serangan yang "cukup berat" sebelum dianggap sebagai serangan bersenjata. Resolusi tersebut tidak pernah mendefinisikan serangan bersenjata, tetapi memberikan contoh yang diterima secara luas oleh komunitas internasional. Meskipun resolusi tersebut telah membantu menyelesaikan arti serangan bersenjata untuk serangan konvensional, semakin maju teknologi, semakin banyak serangan datang dalam bentuk yang sebelumnya tidak tercakup dalam deklarasi dan praktik negara. Akibatnya, negara-negara mengakui bahwa penggunaan kekuatan yang tidak konvensional dapat memerlukan perlakuan sebagai serangan bersenjata ketika ruang lingkup, durasi, dan intensitasnya cukup berat. Akibatnya, negara-negara terus membuat pernyataan tentang

metode perang baru, perlahan-lahan membentuk paradigma untuk mengklasifikasikan serangan bersenjata.

Para ahli telah mengembangkan beberapa model analitik untuk menangani serangan tidak konvensional, seperti serangan dunia maya, untuk membantu memudahkan klasifikasi serangan dan menempatkan analisis cakupan, durasi, dan intensitas ke dalam istilah yang lebih konkret. Model-model ini sangat relevan dengan serangan dunia maya karena berada di antara aktivitas kriminal dan perang bersenjata. Ada tiga model analitik utama untuk menangani serangan tidak konvensional. Model pertama adalah pendekatan berbasis instrumen, yang memeriksa untuk melihat apakah kerusakan yang disebabkan oleh metode serangan baru sebelumnya dapat dicapai hanya dengan serangan kinetik. Yang kedua adalah pendekatan berbasis efek, kadang-kadang disebut pendekatan berbasis konsekuensi, di mana kesamaan serangan dengan serangan kinetik tidak relevan dan fokusnya bergeser ke efek keseluruhan serangan dunia maya terhadap negara korban. Yang ketiga adalah pendekatan pertanggungjawaban ketat, di mana serangan siber terhadap infrastruktur penting secara otomatis diperlakukan sebagai serangan bersenjata, karena konsekuensi parah yang dapat diakibatkan oleh penonaktifan sistem tersebut.

Dari ketiga pendekatan tersebut, pendekatan berbasis efek merupakan model analitis terbaik untuk menghadapi serangan cyber. Analisis berbasis efek tidak hanya menjelaskan semua yang dicakup oleh pendekatan berbasis instrumen, tetapi juga menyediakan kerangka kerja analitis untuk situasi yang tidak sama dengan serangan kinetik. Analisis berbasis efek juga lebih unggul daripada kewajiban ketat karena tanggapan terhadap serangan dunia maya di bawah pendekatan berbasis efek sesuai dengan norma dan kebiasaan hukum yang diterima secara internasional, sedangkan pendekatan kewajiban ketat dapat menyebabkan negara korban melanggar hukum perang.

Dari semua cendekiawan yang menganjurkan model berbasis efek, Michael N. Schmitt telah mengembangkan kerangka kerja analitis yang paling berguna untuk mengevaluasi serangan cyber. Dalam artikel mani "Serangan Jaringan Komputer dan Penggunaan Kekuatan dalam Hukum Internasional: Pemikiran tentang Kerangka Normatif," Schmitt menjabarkan enam kriteria untuk mengevaluasi serangan cyber sebagai serangan bersenjata. Kriteria ini adalah keparahan, kedekatan, keterusterangan, invasif, terukur, dan legitimasi dugaan. Secara bersama-sama, mereka memungkinkan negara untuk mengukur serangan dunia maya di beberapa sumbu yang berbeda. Meskipun tidak ada satu kriteria pun yang tidak positif, serangan siber memenuhi kriteria yang cukup untuk dicirikan sebagai serangan bersenjata. Sejak publikasi mereka, kriteria Schmitt telah mendapatkan daya tarik di komunitas hukum, dengan beberapa sarjana hukum terkemuka mengadvokasi penggunaannya. Banyak yang berharap bahwa kriteria Schmitt akan membantu menyeragamkan upaya negara untuk mengklasifikasikan serangan dunia maya. Namun, sampai kriteria Schmitt mendapatkan penerimaan yang lebih luas, negara cenderung mengklasifikasikan serangan dunia maya secara berbeda, tergantung pada pemahaman mereka tentang serangan bersenjata serta konsepsi mereka tentang kepentingan nasional yang vital.

Mengklasifikasikan serangan dunia maya akan sulit dilakukan oleh negara dalam praktiknya. Meskipun keputusan awal untuk menanggapi serangan dunia maya di bawah hukum perang sebagai masalah kebijakan harus dibuat oleh pembuat kebijakan negara,

keputusan aktual untuk menggunakan pertahanan aktif akan memiliki untuk didorong ke administrator sistem yang benar-benar mengoperasikan jaringan komputer. Salah satu tantangan yang akan dihadapi pembuat kebijakan adalah menerjemahkan hukum internasional ke dalam aturan yang ringkas dan dapat dimengerti untuk diikuti oleh administrator sistem mereka, sehingga agen suatu negara mematuhi hukum internasional sambil melindungi jaringan komputer vitalnya. Namun, mengklasifikasikan serangan dunia maya sebagai serangan bersenjata atau serangan bersenjata yang akan segera terjadi hanyalah rintangan pertama yang harus diselesaikan oleh administrator sistem sebelum merespons dengan pertahanan aktif. Rintangan kedua dan sama pentingnya adalah menetapkan tanggung jawab negara atas serangan itu.

14.9 STUDI KASUS INTERNASIONAL-II

Serangan Cyber sebagai Serangan Bersenjata: Negara korban harus dapat mengklasifikasikan serangan dunia maya sebagai serangan bersenjata atau serangan bersenjata yang akan segera terjadi sebelum merespons dengan pertahanan aktif karena, seperti yang telah kita bahas sebelumnya dalam bab ini, serangan bersenjata dan serangan bersenjata yang akan segera terjadi adalah pemicu yang memungkinkan negara untuk merespon dalam membela diri atau membela diri antisipatif. Idealnya, akan ada aturan yang jelas untuk mengklasifikasikan serangan dunia maya sebagai serangan bersenjata, serangan bersenjata yang akan segera terjadi, atau penggunaan kekuatan yang lebih rendah. Sayangnya, karena serangan dunia maya adalah bentuk serangan yang relatif baru, upaya internasional untuk mengklasifikasikannya masih dalam tahap awal, meskipun prinsip-prinsip hukum inti yang mengatur serangan bersenjata telah ditetapkan dengan baik. Akibatnya, apakah serangan siber dapat dikualifikasikan sebagai serangan bersenjata dan serangan siber mana yang harus dianggap sebagai serangan bersenjata masih menjadi pertanyaan terbuka dalam hukum internasional. Untuk menjawab pertanyaan-pertanyaan ini, subbagian ini mengkaji prinsip-prinsip hukum inti yang mengatur serangan bersenjata, menerapkannya pada serangan dunia maya, menjelaskan mengapa serangan dunia maya dapat dikualifikasikan sebagai serangan bersenjata, dan upaya untuk memberikan beberapa wawasan tentang serangan dunia maya mana yang harus dianggap sebagai serangan bersenjata.

"Serangan bersenjata" tidak didefinisikan oleh konvensi internasional mana pun. Akibatnya, maknanya dibiarkan terbuka untuk interpretasi oleh negara dan ulama. Meskipun ini mungkin terdengar bermasalah, sebenarnya tidak. Kerangka kerja untuk menganalisis serangan bersenjata relatif sudah mapan, seperti prinsip-prinsip hukum inti yang mengatur maknanya. Masyarakat internasional umumnya menerima uji ruang lingkup, durasi, dan intensitas Jean S. Pictet sebagai titik awal untuk mengevaluasi apakah penggunaan kekuatan tertentu merupakan serangan bersenjata. Di bawah uji Pictet, penggunaan kekuatan adalah serangan bersenjata jika cakupan, durasi, dan intensitasnya cukup. Tentu saja, seperti halnya dengan banyak konsep hukum internasional, negara, organisasi non-pemerintah, dan para sarjana semua menafsirkan ruang lingkup, durasi, dan uji intensitas secara berbeda.

Deklarasi negara membantu menyempurnakan penggunaan kekuatan mana yang memiliki cakupan, durasi, dan intensitas yang cukup untuk membentuk serangan bersenjata.

Mengingat kembali Piagam PBB versi bahasa Prancis, yang mengacu pada "agresi bersenjata" daripada "serangan bersenjata", Majelis Umum PBB mengeluarkan resolusi Definisi Agresi pada tahun 1974. Resolusi tersebut mensyaratkan serangan harus "gravitasi yang cukup" sebelum dianggap sebagai serangan bersenjata. Resolusi tersebut tidak pernah mendefinisikan serangan bersenjata, tetapi memberikan contoh yang diterima secara luas oleh komunitas internasional.

Meskipun resolusi tersebut telah membantu menyelesaikan arti serangan bersenjata untuk serangan konvensional, semakin maju teknologi, semakin banyak serangan datang dalam bentuk yang sebelumnya tidak tercakup dalam deklarasi dan praktik negara. Akibatnya, negara-negara mengakui bahwa penggunaan kekuatan yang tidak konvensional dapat memerlukan perlakuan sebagai serangan bersenjata ketika ruang lingkup, durasi, dan intensitasnya cukup berat. Akibatnya, negara-negara terus membuat pernyataan tentang metode perang baru, perlahan-lahan membentuk paradigma untuk mengklasifikasikan serangan bersenjata.

Para ahli telah mengembangkan beberapa model analitik untuk menangani serangan tidak konvensional, seperti serangan dunia maya, untuk membantu memudahkan klasifikasi serangan dan menempatkan analisis cakupan, durasi, dan intensitas ke dalam istilah yang lebih konkret. Model-model ini sangat relevan dengan serangan dunia maya karena berada di antara aktivitas kriminal dan perang bersenjata. Ada tiga model analitik utama untuk menangani serangan tidak konvensional. Model pertama adalah pendekatan berbasis instrumen, yang memeriksa untuk melihat apakah kerusakan yang disebabkan oleh metode serangan baru sebelumnya dapat dicapai hanya dengan serangan kinetik. Yang kedua adalah pendekatan berbasis efek, kadang-kadang disebut pendekatan berbasis konsekuensi, di mana kesamaan serangan dengan serangan kinetik tidak relevan dan fokusnya bergeser ke efek keseluruhan serangan dunia maya terhadap negara korban. Yang ketiga adalah pendekatan pertanggungjawaban ketat, di mana serangan siber terhadap infrastruktur penting secara otomatis diperlakukan sebagai serangan bersenjata, karena konsekuensi parah yang dapat diakibatkan oleh penonaktifan sistem tersebut.

Dari ketiga pendekatan tersebut, pendekatan berbasis efek merupakan model analitis terbaik untuk menghadapi serangan cyber. Analisis berbasis efek tidak hanya menjelaskan semua yang dicakup oleh pendekatan berbasis instrumen, tetapi juga menyediakan kerangka kerja analitis untuk situasi yang tidak sama dengan serangan kinetik. Analisis berbasis efek juga lebih unggul daripada kewajiban ketat karena tanggapan terhadap serangan dunia maya di bawah pendekatan berbasis efek sesuai dengan norma dan kebiasaan hukum yang diterima secara internasional, sedangkan pendekatan kewajiban ketat dapat menyebabkan negara korban melanggar hukum perang.

Dari semua cendekiawan yang menganjurkan model berbasis efek, Michael N. Schmitt telah mengembangkan kerangka kerja analitis yang paling berguna untuk mengevaluasi serangan cyber. Dalam artikel mani "Serangan Jaringan Komputer dan Penggunaan Kekuatan dalam Hukum Internasional: Pemikiran tentang Kerangka Normatif," Schmitt menjabarkan enam kriteria untuk mengevaluasi serangan cyber sebagai serangan bersenjata. Kriteria ini adalah keparahan, kedekatan, keterusterangan, invasif, terukur, dan legitimasi dugaan. Secara bersama-sama, mereka memungkinkan negara untuk mengukur serangan dunia maya di

beberapa sumbu yang berbeda. Meskipun tidak ada satu kriteria pun yang dispositif, serangan siber memenuhi kriteria yang cukup untuk menjadi dicirikan sebagai serangan bersenjata. Sejak publikasi mereka, kriteria Schmitt telah mendapatkan daya tarik di komunitas hukum, dengan beberapa sarjana hukum terkemuka mengadvokasi penggunaannya. Banyak yang berharap bahwa kriteria Schmitt akan membantu menyeragamkan upaya negara untuk mengklasifikasikan serangan dunia maya. Namun, sampai kriteria Schmitt mendapatkan penerimaan yang lebih luas, negara cenderung mengklasifikasikan serangan dunia maya secara berbeda, tergantung pada pemahaman mereka tentang serangan bersenjata serta konsepsi mereka tentang kepentingan nasional yang vital.

Mengklasifikasikan serangan siber akan sulit dilakukan oleh negara dalam praktiknya. Meskipun keputusan awal untuk menanggapi serangan cyber di bawah hukum perang sebagai masalah kebijakan harus dibuat oleh pembuat kebijakan negara, keputusan sebenarnya untuk menggunakan pertahanan aktif harus didorong ke administrator sistem yang benar-benar mengoperasikan jaringan komputer. . Salah satu tantangan yang akan dihadapi pembuat kebijakan adalah menerjemahkan hukum internasional ke dalam aturan yang ringkas dan dapat dimengerti untuk diikuti oleh administrator sistem mereka, sehingga agen suatu negara mematuhi hukum internasional sambil melindungi jaringan komputer vitalnya. Namun, mengklasifikasikan serangan dunia maya sebagai serangan bersenjata atau serangan bersenjata yang akan segera terjadi hanyalah rintangan pertama yang harus diselesaikan oleh administrator sistem sebelum merespons dengan pertahanan aktif. Rintangan kedua dan sama pentingnya adalah menetapkan tanggung jawab negara atas serangan itu.

14.10 STUDI KASUS INTERNASIONAL-III

Black Ice: The Invisible Threat of Cyber-Terror, sebuah buku yang diterbitkan pada tahun 2003 dan ditulis oleh jurnalis Computerworld dan mantan perwira intelijen Dan Verton, menjelaskan latihan tahun 1997 dengan kode nama "Penerima yang Memenuhi Syarat," yang dilakukan oleh National Security Agency (NSA). (Akun berikut diambil dari "Black Ice," Computerworld, 13 Agustus 2003.) Latihan dimulai ketika pejabat NSA menginstruksikan "Tim Merah" yang terdiri dari tiga puluh lima peretas untuk mencoba meretas dan mengganggu sistem keamanan nasional AS. Mereka diminta untuk berperan sebagai peretas yang disewa oleh dinas intelijen Korea Utara, dan target utama mereka adalah Komando Pasifik AS di Hawaii. Mereka diizinkan untuk menembus jaringan Pentagon mana pun tetapi dilarang melanggar undang-undang AS, dan mereka hanya dapat menggunakan perangkat lunak peretasan yang dapat diunduh secara bebas dari Internet. Mereka mulai memetakan jaringan dan memperoleh kata sandi yang diperoleh melalui "brute-force cracking" (metode coba-coba untuk memecahkan kode data terenkripsi seperti kata sandi atau kunci enkripsi dengan mencoba semua kemungkinan kombinasi). Seringkali mereka menggunakan taktik yang lebih sederhana seperti menelepon seseorang, berpura-pura menjadi teknisi atau pejabat tinggi, dan meminta kata sandi. Para peretas berhasil mendapatkan akses ke lusinan sistem komputer Pentagon yang kritis.

Begitu mereka memasuki sistem, mereka dapat dengan mudah membuat akun pengguna, menghapus akun yang ada, memformat ulang hard drive, mengacak data yang tersimpan, atau mematikan sistem. Mereka memecahkan pertahanan jaringan dengan relatif

mudah dan melakukannya tanpa dilacak atau diidentifikasi oleh pihak berwenang. Hasilnya mengejutkan penyelenggara. Pertama-tama, Tim Merah telah menunjukkan bahwa adalah mungkin untuk membobol sistem komando dan kontrol militer Pasifik AS dan, berpotensi melumpuhkannya. Kedua, pejabat NSA yang memeriksa hasil eksperimen menemukan bahwa banyak infrastruktur sektor swasta di Amerika Serikat, seperti telekomunikasi dan jaringan listrik, dapat dengan mudah diserbu dan disalahgunakan dengan cara yang sama. Kerentanan industri energi adalah inti dari Black Ice.

Verton berpendapat bahwa sektor energi Amerika akan menjadi domino pertama yang jatuh dalam serangan teroris cyber strategis terhadap Amerika Serikat. Buku ini mengeksplorasi dengan detail yang menakutkan bagaimana dampak serangan semacam itu dapat menyaingi, atau bahkan melebihi, konsekuensi dari serangan fisik yang lebih tradisional. Verton mengklaim bahwa selama tahun tertentu, rata-rata perusahaan utilitas besar di Amerika Serikat mengalami sekitar 1 juta intrusi dunia maya. Data yang dikumpulkan oleh Riptech, Inc.—perusahaan berbasis di Virginia yang mengkhususkan diri dalam keamanan informasi online dan sistem keuangan—tentang serangan siber selama enam bulan setelah serangan 9/11 menunjukkan bahwa perusahaan-perusahaan di industri energi mengalami gangguan dua kali lipat lebih cepat. industri lain, dengan jumlah serangan berat atau kritis yang membutuhkan intervensi segera rata-rata 12,5 per perusahaan.

Pada tahun 1997, sebuah organisasi teroris Bolivia telah membunuh empat personel tentara AS. Sebuah serangan di salah satu tempat persembunyian teroris menghasilkan informasi yang dienkripsi menggunakan enkripsi simetris. Serangan brute force 12 jam mengakibatkan dekripsi informasi dan kemudian menyebabkan salah satu penangkapan narkoba terbesar dalam sejarah Bolivia dan penangkapan para teroris.

Pada tahun 1999 hacker menyerang komputer NATO. Komputer membanjiri mereka dengan email dan menyerang mereka dengan penolakan layanan (DoS). Para peretas memprotes pengeboman NATO di Kosovo. Bisnis, organisasi publik, dan institusi akademik dibombardir dengan email yang sangat dipolitisasi yang berisi virus dari negara-negara Eropa lainnya.

Pada tahun 2001, di balik penurunan hubungan AS-China, para peretas China merilis virus Code Red ke alam liar. Virus ini menginfeksi jutaan komputer di seluruh dunia dan kemudian menggunakan komputer ini untuk meluncurkan serangan penolakan layanan di situs web AS, terutama situs web Gedung Putih. Pada tahun 2002, banyak situs web terkemuka India dirusak. Pesan-pesan yang berkaitan dengan masalah Kashmir ditempelkan di halaman utama situs web ini. Klub Hackerz Pakistan, yang dipimpin oleh "Dokter Neukar" diyakini berada di balik serangan ini.

Pada Mei 2007 Estonia menjadi sasaran serangan cyber massal oleh peretas di dalam Federasi Rusia yang menurut beberapa bukti dikoordinasikan oleh pemerintah Rusia, meskipun pejabat Rusia menyangkal mengetahui hal ini. Serangan ini tampaknya sebagai tanggapan atas pemindahan tugu peringatan Perang Dunia II Rusia dari pusat kota Estonia.

Pada bulan Desember 2010, situs web Biro Pusat Investigasi (CBI) diretas oleh pemrogram yang mengidentifikasi diri mereka sebagai "Tentara Cyber Pakistan".

14.11 RINGKASAN

Serangan siber adalah salah satu ancaman terbesar bagi perdamaian dan keamanan internasional di abad ke-21. Mengamankan dunia maya adalah keharusan mutlak. Di dunia yang ideal, negara-negara akan bekerja sama untuk menghilangkan ancaman dunia maya. Sayangnya, dunia kita bukanlah utopia, juga tidak mungkin menjadi satu. Kerja sama global mungkin menjadi kenyataan suatu hari nanti, tetapi kecuali ada sesuatu yang berubah untuk menekan negara-negara suaka agar mengubah perilaku mereka, tidak ada dorongan bagi mereka untuk melakukannya. Cara untuk mencapai kenyataan ini adalah dengan menggunakan pertahanan aktif terhadap serangan siber yang berasal dari negara suaka. Hal ini tidak hanya akan memungkinkan negara-negara korban untuk melindungi diri mereka sendiri dengan lebih baik dari serangan dunia maya, tetapi juga harus mencegah agresi dan mendorong negara-negara suaka untuk menjalankan tugas internasional mereka dengan serius. Lagi pula, tidak ada negara yang menginginkan negara lain menggunakan kekuatan di dalam perbatasannya, bahkan secara elektronik.

Dengan demikian, kemungkinan bahwa serangan siber akan mendapat respons yang kuat adalah palu yang dapat mendorong akal sehat ke negara-negara suaka. Dalam unit ini konsep penting terorisme dunia maya dalam perspektif global, upaya hukum internasional, penindasan pendanaan terorisme, tindakan PBB untuk melawan terorisme, terorisme dunia maya yaitu kejahatan dunia maya, perang dunia maya dan terorisme dunia maya dan studi kasus internasional dibahas panjang lebar untuk kejelasan yang lebih baik untuk memahami masalah yang terkait dengan terorisme dunia maya secara global.

14.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Authorpress)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)

- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang tepat dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

14.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Terorisme dunia maya adalah penggunaan kegiatan yang mengganggu secara terencana.
b) Konsep dan metode tradisional terorisme telah mengambil dimensi baru, yang sifatnya lebih destruktif dan mematikan.
c) Negara-negara diminta untuk bertukar informasi dan bekerja sama untuk mencegah dan menekan tindakan teroris dan untuk mengambil tindakan.
d) Resolusi PBB No. 1373 (2001) diadopsi dengan suara bulat pada tanggal 28 September 2001.
e) Kelompok teroris semakin paham komputer dan beberapa mungkin memperoleh kemampuan untuk menggunakan serangan dunia maya.

B. Isi Bagian yang Kosong:

I. Resolusi PBB No.....terkait dengan pemberantasan terorisme secara global.
II. Jarak.....jarak antara penyerang dan korban dan kesulitan melacak kembali serangan.
III. .....biasanya memiliki arti yang lebih kuat dari kejahatan dunia maya.
IV. Istilah seperti..... dan "terorisme dunia maya" telah banyak digunakan di media.
V. Sangat sulit untuk mengetahui secara pasti siapa dalang di balik.....dan motif mereka.

14.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. 1.1371 tahun 2001
2. Virtual dan fisik
3. Terorisme Dunia Maya
4. Perang Cyber

5. Serangan dunia maya

14.15 PERTANYAAN TERMINAL

1. Apa definisi global dari terorisme dunia maya?
2. Menentukan tindakan PBB untuk melawan terorisme.
3. Definisikan terorisme cyber yaitu kejahatan dunia maya.
4. Apa itu perang siber dan terorisme siber?
5. Diskusikan dua studi kasus internasional.

BAB 15
TERORISME CYBER: PERSPEKTIF INDIA

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan Terorisme Cyber dalam Perspektif India
- Memahami sifat dan ruang lingkup Ketentuan-Ketentuan Statuta Penting
- Memahami masalah teknis dan hukum terkait dengan Terorisme Cyber dengan mengacu pada Perspektif India

15.1 PENGANTAR

Ancaman yang ditimbulkan oleh terorisme siber telah menarik perhatian media massa, komunitas keamanan, dan industri teknologi informasi (TI).

Jurnalis, politisi, dan pakar di berbagai bidang telah mempopulerkan skenario di mana teroris dunia maya yang canggih secara elektronik membobol komputer yang mengendalikan bendungan atau sistem kontrol lalu lintas udara, mendatangkan malapetaka dan membahayakan tidak hanya jutaan nyawa tetapi juga keamanan nasional itu sendiri. Namun, terlepas dari semua prediksi suram tentang hari kiamat yang dihasilkan dunia maya, tidak ada satu pun contoh terorisme dunia maya nyata yang tercatat. Seberapa nyata ancaman yang ditimbulkan oleh terorisme dunia maya? Karena infrastruktur yang paling penting dalam masyarakat Barat adalah jaringan melalui komputer, potensi ancaman dari terorisme dunia maya, tentu saja, sangat mengkhawatirkan. Peretas, meskipun tidak termotivasi oleh tujuan yang sama yang menginspirasi teroris, telah menunjukkan bahwa individu dapat memperoleh akses ke informasi sensitif dan pengoperasian layanan penting.

Teroris, setidaknya secara teori, dapat mengikuti jejak para peretas dan kemudian, setelah membobol sistem komputer pemerintah dan swasta, melumpuhkan atau setidaknya melumpuhkan sektor militer, keuangan, dan layanan di negara-negara maju. Meningkatnya ketergantungan masyarakat kita pada teknologi informasi telah menciptakan bentuk kerentanan baru, memberikan teroris kesempatan untuk mendekati target yang seharusnya tidak dapat disangkal, seperti sistem pertahanan nasional dan sistem kontrol lalu lintas udara. Semakin maju teknologi suatu negara, semakin rentan terhadap serangan siber terhadap infrastrukturnya. Kekhawatiran tentang potensi bahaya yang ditimbulkan oleh terorisme dunia maya sangat beralasan. Namun, itu tidak berarti bahwa semua ketakutan yang telah disuarakan di media, di Kongres, dan di forum publik lainnya adalah rasional dan masuk akal. Beberapa ketakutan tidak dapat dibenarkan, sementara yang lain sangat dibesar-besarkan. Selain itu, perbedaan antara potensi dan kerusakan aktual yang ditimbulkan oleh teroris siber terlalu sering diabaikan, dan aktivitas sebagian besar peretas yang relatif tidak berbahaya telah digabungkan dengan momok terorisme siber murni.

15.2 TERORISME CYBER: ARTI DAN DEFINISI MENURUT HUKUM INDIA

Terorisme dunia maya adalah penggunaan kegiatan yang mengganggu atau ancamannya secara terencana, di ruang maya, dengan maksud untuk memajukan tujuan sosial, ideologis, agama, politik atau serupa, atau untuk mengintimidasi siapa pun dalam memajukan tujuan tersebut. Komputer dan internet menjadi bagian penting dari kehidupan kita sehari-hari. Mereka digunakan oleh individu dan masyarakat untuk membuat hidup mereka lebih mudah.

Mereka menggunakannya untuk menyimpan informasi, memproses data, mengirim dan menerima pesan, komunikasi, mengendalikan mesin, mengetik, mengedit, mendesain, menggambar, dan hampir semua aspek kehidupan.

Akibat paling mematikan dan destruktif dari ketidakberdayaan ini adalah munculnya konsep “cyber terrorism”. Konsep dan metode tradisional terorisme telah mengambil dimensi baru, yang sifatnya lebih destruktif dan mematikan. Di era teknologi informasi para teroris telah memperoleh keahlian untuk menghasilkan kombinasi senjata dan teknologi yang paling mematikan, yang jika tidak dijaga dengan baik pada waktunya, akan memakan korbannya sendiri. Kerusakan yang dihasilkan akan hampir tidak dapat diubah dan paling bencana di alam. Singkatnya, kita menghadapi bentuk terorisme terburuk yang dikenal sebagai "Terorisme Cyber". Ungkapan "terorisme dunia maya" mencakup penggunaan negatif dan berbahaya yang disengaja dari teknologi informasi untuk menghasilkan efek yang merusak dan merugikan properti, baik berwujud maupun tidak berwujud, milik orang lain. Misalnya, meretas sistem komputer dan kemudian menghapus informasi bisnis yang berguna dan berharga dari pesaing saingan adalah bagian tak terpisahkan dari terorisme dunia maya.

Definisi "terorisme dunia maya" tidak dapat dibuat lengkap karena sifat kejahatannya sedemikian rupa sehingga harus dibiarkan bersifat inklusif. Sifat "dunia maya" sedemikian rupa sehingga metode dan teknologi baru ditemukan secara teratur; maka tidak disarankan untuk menempatkan definisi dalam formula straightjacket atau merpati utuh. Padahal, upaya pertama yang harus dilakukan Pengadilan adalah menafsirkan definisi tersebut sebebas mungkin sehingga ancaman terorisme dunia maya dapat ditangani secara tegas dan dengan hukuman yang berat.

Undang-undang yang menangani terorisme dunia maya, bagaimanapun, tidak cukup untuk memenuhi niat berbahaya para teroris dunia maya ini dan membutuhkan peremajaan dalam konteks dan perkembangan terbaru di seluruh dunia. Definisi Terorisme Cyber: Sebelum kita dapat membahas kemungkinan "terorisme dunia maya, kita harus memiliki beberapa definisi kerja. Kata "terorisme dunia maya" mengacu pada dua elemen: dunia maya dan terorisme.

Kata lain dari dunia maya adalah "dunia maya" yaitu tempat di mana program komputer berfungsi dan data bergerak. Terorisme adalah istilah yang banyak digunakan, dengan banyak definisi. Untuk keperluan presentasi ini, kami akan menggunakan definisi Departemen Luar Negeri Amerika Serikat: "Istilah 'terorisme' berarti kekerasan yang direncanakan dan bermotivasi politik yang dilakukan terhadap sasaran non-pejuang oleh kelompok sub-nasional atau agen klandestin."

Jika kita menggabungkan definisi ini, kita membangun definisi kerja seperti berikut: "Terorisme dunia maya adalah serangan yang direncanakan, bermotivasi politik terhadap

informasi, sistem komputer, program komputer, dan data yang mengakibatkan kekerasan terhadap target non-kombatan oleh kelompok sub-nasional atau klandestin agen.

Definisi dasar Terorisme dunia maya dimasukkan dari waktu ke waktu untuk mencakup hal-hal seperti sekadar merusak situs web atau server, atau menyerang sistem yang tidak kritis, yang mengakibatkan istilah tersebut menjadi kurang berguna. Ada juga aliran pemikiran yang mengatakan terorisme cyber tidak ada dan benar-benar masalah peretasan atau perang informasi. Beberapa tidak setuju dengan pelabelan terorisme yang tepat karena kecilnya kemungkinan terciptanya ketakutan akan bahaya fisik yang signifikan atau kematian dalam populasi yang menggunakan sarana elektronik, mengingat serangan saat ini dan teknologi perlindungan.

Cyber Terrorism and IT Act, 2000:

Amandemen di bawah Undang-Undang Teknologi Informasi, 2000 telah mendefinisikan istilah "Terorisme siber" U/Sec. 66F. Ini adalah upaya pertama di India untuk mendefinisikan istilah tersebut. Bunyinya seperti di bawah ini: -

Hukuman untuk terorisme Cyber: Siapa pun:

A. dengan maksud untuk mengancam persatuan, integritas, keamanan atau kedaulatan India atau untuk melakukan teror terhadap orang-orang atau bagian mana pun dari orang-orang dengan—
    i) menolak atau menyebabkan penolakan akses ke setiap orang yang berwenang untuk mengakses sumber daya komputer; atau
    ii) mencoba menembus atau mengakses sumber daya komputer tanpa izin atau melebihi akses yang diizinkan; atau
    iii) memperkenalkan atau menyebabkan masuknya kontaminan komputer; dan melalui tindakan tersebut menyebabkan atau kemungkinan besar menyebabkan kematian atau cedera pada orang atau kerusakan atau penghancuran properti atau mengganggu atau mengetahui bahwa hal itu mungkin menyebabkan kerusakan atau gangguan pasokan atau layanan yang penting bagi kehidupan masyarakat atau merugikan mempengaruhi infrastruktur informasi penting yang ditentukan dalam Bagian 70, atau
B. dengan sadar atau sengaja menembus atau mengakses sumber daya komputer tanpa izin atau melebihi akses yang diizinkan, dan dengan cara tersebut memperoleh akses ke informasi, data atau basis data komputer yang dibatasi untuk alasan keamanan Negara atau hubungan luar negeri, atau informasi, data, atau basis data komputer apa pun yang dibatasi, dengan alasan untuk meyakini bahwa informasi, data, atau basis data komputer tersebut yang diperoleh dapat digunakan untuk menyebabkan atau mungkin menyebabkan kerugian bagi kepentingan kedaulatan dan integritas India, keamanan Negara, hubungan persahabatan dengan negara asing, ketertiban umum, kesusilaan atau moralitas, atau dalam kaitannya dengan penghinaan terhadap pengadilan, pencemaran nama baik atau hasutan untuk melakukan pelanggaran, atau untuk keuntungan negara asing, kelompok individu atau lainnya, melakukan pelanggaran terorisme dunia maya.

Hukuman: Siapa pun yang melakukan atau bersekongkol untuk melakukan terorisme dunia maya diancam dengan hukuman penjara yang dapat diperpanjang hingga penjara seumur hidup. Yaitu. Penjara tidak lebih dari empat belas tahun (Bag. 55, IPC) Bagian ini telah mendefinisikan serangan Cyber konvensional seperti, akses tidak sah, serangan penolakan

layanan, dll, tetapi seperti yang dibahas di atas, motif dan niat pelaku membedakan serangan dari biasa ke tindakan terorisme.

Ilustrasi: Rohit, seorang Peretas, mendapatkan akses tidak sah ke jaringan kontrol lalu lintas Kereta Api (jaringan telah dinyatakan sebagai Infrastruktur Informasi Kritis U/Sec. 70) dan dengan demikian menyerang teror di antara orang-orang, Rohit dikatakan telah melakukan tindakan terorisme Cyber.

15.3 TERORISME CYBER DAN KUHP INDIA, 1860

Situs web India adalah target baru peretas: Beberapa ahli komputer berhasil membobol jaringan komputer dengan keamanan tinggi dari Pusat Penelitian Atom Bhabha tetapi untungnya terdeteksi. ''GForce,'' sekelompok peretas anonim yang anggotanya menulis slogan-slogan kritis terhadap India dan klaimnya atas Kashmir, telah memiliki beberapa contoh peretasan situs India yang dijalankan oleh pemerintah India, perusahaan swasta, atau organisasi ilmiah. Kepala NAASCOM mengatakan perusahaan India rata-rata hanya menghabiskan 0,8 persen dari anggaran teknologi mereka untuk keamanan, dibandingkan rata-rata global 5,5 persen. Sejumlah kasus peretasan situs internet India telah dilacak ke Pakistan tetapi akan sulit untuk menangkapnya, kata Direktur CBI, R K Ragavan. Karena para peretas yang membobol sistem komputer di India tidak berkomplot dengan penegak hukum Pakistan, ''Orang bertanya-tanya kerjasama macam apa yang akan kita dapatkan'' kata Ragavan dalam sebuah seminar tentang keamanan Internet. Peretas yang menggunakan pengetahuan perangkat lunak untuk membobol dan mencuri informasi dari sistem komputer membobol setidaknya 635 situs internet India tahun lalu. Mr Raghavan mengatakan kebangkitan melek huruf di India dapat menurunkan kejahatan konvensional tetapi kerentanan komputer dan Internet dapat membuat kejahatan melalui media lebih merajalela.

''Kami di CBI yakin bahwa kejahatan dunia maya adalah kejahatan masa depan,'' katanya. ''Sekarang jauh lebih mudah dilakukan dan kurang mudah diidentifikasi.''Presiden Asosiasi Perusahaan Perangkat Lunak dan Layanan Nasional India (NASSCOM), Dewang Mehta mengatakan kurangnya undang-undang yang seragam terhadap kejahatan dunia maya yang melibatkan penyalahgunaan sistem komputer membuat penuntutan lintas -peretas perbatasan sulit. ''Peretasan bukanlah pelanggaran universal, dan ada masalah,'' kata Mr Mehta.

Tahun lalu, India mengesahkan undang-undang digital penting yang membuat peretasan, penyebaran virus, dan transaksi keuangan ilegal melalui Internet dapat dihukum. Itu menjadi anggota ke-12 di klub kecil negara-negara dengan hukum digital.

Dilaporkan bahwa Pakistan menggunakan sistem komputer untuk mempromosikan terorisme di India. Ini hanya beberapa contoh yang dikutip oleh Bhure Lal, sekretaris di Komisi Kewaspadaan Pusat, untuk membuat alasan yang kuat untuk penerapan undang-undang dunia maya. Dia berbicara pada seminar nasional tentang Kejahatan Terkait Komputer yang diselenggarakan oleh Biro Pusat Investigasi (CBI) di Ibukota hari ini. Menggarisbawahi perlunya undang-undang dunia maya yang komprehensif, ia menambahkan bahwa penyalahgunaan komputer juga dapat digunakan untuk terorisme dunia maya.

Untuk mengembangkan perlindungan yang efektif terhadap ancaman kejahatan komputer, pakar lain dari berbagai lembaga investigasi, termasuk Biro Investigasi Federal (FBI)

dan Interpol, hari ini mencari undang-undang dunia maya yang spesifik dan komprehensif untuk mencakup semua tindakan penjahat komputer dan mekanisme proaktif untuk menanganinya. pelanggaran seperti itu.

"Tidak hanya sulit untuk mendeteksi kejahatan komputer, tetapi juga untuk menangkap penjahat karena undang-undang tidak mengikuti perkembangan teknologi," kata Deputi Gubernur Reserve Bank of India S.P. Talwar.

Menekankan perlunya fitur keamanan yang efektif saat melakukan komputerisasi, dia berkata ``Seringkali sulit untuk menghubungkan kesalahan menggunakan undang-undang yang ada karena tindakan masuk tanpa izin ke dalam sistem dan merusak data virtual mungkin tidak secara khusus diatur dalam undang-undang.' Dalam sambutannya, Direktur CBI (Mantan) R.K. Raghavan mengatakan pemerintah menyadari perlunya undang-undang di bidang baru teknologi informasi ini dan oleh karena itu, Departemen Elektronik (DoE) berkonsultasi dengan lembaga ahli lainnya telah menyusun undang-undang yang berkaitan dengan bidang ini. Menyadari ancaman kejahatan komputer, CBI telah mengambil ``proaktif'' memimpin dalam mempersiapkan diri untuk menghadapi tantangan dengan membentuk Unit Kejahatan Cyber khusus, katanya.

RBI juga dikaitkan dengan upaya kementerian Keuangan, Perdagangan dan Hukum dalam pengesahan undang-undang seperti Undang-Undang Teknologi Informasi dan Undang-Undang Cyber, kata Talwar.

Pada saat yang sama, ia menambahkan bahwa kecuali pengembangan fitur keamanan juga diperhatikan pada tingkat efisiensi dan kecepatan yang sama, bank akan dibiarkan dengan ``sistem perangkat lunak yang indah untuk silau dan akses publik, tetapi sama sekali tidak dijaga dan mudah tertipu terhadap informasi yang menunggu. pemburu''.

SMS ofensif dapat menyebabkan 2 tahun penjara

Dengan telepon seluler dan telepon seluler prabayar yang secara virtual mengambil alih peran komputer pribadi, amandemen yang diusulkan pada Undang-Undang Teknologi Informasi, 2006, telah memperjelas bahwa transmisi teks, audio, atau video apa pun yang menyinggung atau memiliki karakter mengancam dapat menjebloskan pengguna ponsel ke penjara selama dua tahun. Hukuman juga akan dikenakan jika kontennya salah dan telah dikirimkan dengan tujuan menyebabkan gangguan, ketidaknyamanan, bahaya, atau penghinaan. Dan jika ponsel tersebut digunakan untuk menipu seseorang melalui penyamaran, maka pelakunya dapat dipidana dengan pidana penjara selama lima tahun.

Kebutuhan untuk mendefinisikan perangkat komunikasi di bawah amandemen yang diusulkan menjadi penting karena undang-undang saat ini tidak menyebutkan perangkat apa yang dapat dimasukkan dalam kategori ini. UU IT yang diamandemen telah mengklarifikasi bahwa ponsel atau bantuan digital pribadi dapat disebut sebagai perangkat komunikasi dan tindakan dapat dimulai sesuai dengan itu. Ditekankan oleh berbagai skandal yang melanda negara itu selama dua tahun terakhir, termasuk penangkapan CEO portal terkenal, pemerintah juga telah memperkenalkan kejahatan dunia maya baru di bawah undang-undang yang diusulkan. Undang-undang yang diubah, yang ditempatkan di hadapan Lok Sabha selama sesi musim dingin yang baru saja berakhir, telah mengecualikan tanggung jawab penyedia layanan jaringan sehubungan dengan tindakan pihak ketiga. Namun, hal itu telah membuat penguntitan dunia maya, pencemaran nama baik dunia maya, dan gangguan dunia maya

sebagai pelanggaran. Siapa pun yang ditemukan terlibat dalam semua pelanggaran ini dapat dipenjara selama dua tahun. Perubahan yang diusulkan juga meminta amandemen dalam bentuk penyisipan dalam KUHP India, sehingga menyatakan pencurian identitas sebagai pelanggaran. Jika seseorang menipu dengan menggunakan tanda tangan elektronik, kata sandi, atau fitur identifikasi unik lainnya dari orang lain, ia akan dihukum dengan hukuman penjara selama dua tahun dan juga dapat dikenakan denda.

Meminta untuk dimasukkan dalam KUHP India sebagai Bagian 502A dari undang-undang, amandemen yang diusulkan telah mengatakan bahwa siapa pun yang dengan sengaja atau sadar menangkap, menerbitkan atau mengirimkan gambar area pribadi seseorang tanpa persetujuannya, akan dihukum dengan penjara dua tahun dan denda Rp 2 juta. Bagian pribadi dapat berupa area publik yang telanjang atau pakaian dalam. Membuat undang-undang lebih netral secara teknologi, ketentuan yang diubah telah memasukkan otentikasi catatan elektronik dengan teknik elektronik apa pun. Saat ini, arsip elektronik dapat diautentikasi hanya dengan tanda tangan digital, teknologi infrastruktur kunci publik (PKI). Dengan ketentuan baru, bagaimanapun, faktor biometrik seperti sidik jari atau retina mata harus dimasukkan sebagai teknik untuk otentikasi. Bahkan ketika pembuat undang-undang telah mencoba untuk menutupi penyimpangan dari UU IT saat ini, mereka tampaknya telah membuatnya liberal dengan mengurangi hukuman dari tiga tahun menjadi dua tahun. Dengan perubahan ini, penjahat dunia maya sekarang berhak mendapatkan jaminan sebagai haknya, saat dan saat dia ditangkap.

15.4 TERORISME CYBER DI INDIA DAN SOLUSINYA

Ancaman terorisme dunia maya bukan hanya tanggung jawab Negara dan perangkatnya. Warga negara serta netizen sama-sama memiliki kewajiban serius untuk memerangi terorisme dunia maya. Padahal, mereka adalah mekanisme pemberantasan dan pemberantasan terorisme siber yang paling penting dan efektif. Satu-satunya persyaratan adalah mendorong mereka untuk maju ke depan untuk mendukung memerangi terorisme dunia maya. Pemerintah dapat memberikan insentif yang sesuai kepada mereka dalam bentuk penghargaan berupa uang. Namun, harus dicatat bahwa anonimitas dan keamanan mereka harus dipastikan sebelum meminta bantuan mereka.

Pengadilan juga diberdayakan untuk menjaga anonimitas mereka jika mereka memberikan informasi dan bukti apa pun untuk memerangi terorisme dunia maya. Masalah cyber terrorism bersifat multilateral yang memiliki berbagai segi dan dimensi. Solusinya membutuhkan penerapan energi dan sumber daya yang ketat. Harus dicatat bahwa hukum selalu tujuh langkah di belakang teknologi. Ini karena kita memiliki kecenderungan untuk membuat undang-undang ketika masalah mencapai puncaknya. Kami tidak menghargai perlunya waktu sampai masalah mengambil dimensi genting. Pada tahap itu selalu sangat sulit, jika bukan tidak mungkin, untuk mengatasi masalah itu. Apalagi jika terjadi pelanggaran dan pelanggaran yang melibatkan teknologi informasi. Undang-undang yang tepat waktu dan tepat selalu merupakan langkah maju yang baik untuk memerangi terorisme dunia maya. India harus menutupi celah panjang sebelum dapat mengamankan batas-batas tradisional dan ruang sibernya.

15.5 STUDI KASUS-I

Hukum dunia maya perlu mengikuti perubahan teknologi, dengan fokus pada internet seluler dan penyalahgunaan media sosial untuk mendefinisikan kembali teror dunia maya, perang, atau naxalisme: Penangkapan Mehdi Masoor Biswas, pria di balik akun Twitter yang menangani @ShamiWitness, sebagai “penumpang ISIS” dan “terduga jihadi” mengajukan pertanyaan tentang apakah tweeting merupakan tindakan teror di hadapan pengadilan hukum India. Ketika sampai pada hal itu, ini bukan tentang "klaim polisi" atau "sumber intelijen", tetapi tentang fakta keras, bukti, dan surat hukum untuk menjawab betapa "terlibatnya teror" tweeter dan tweet hist itu.

Salah satu petugas polisi yang menginterogasi Mehdi mengakui bahwa ini adalah "kasus uji" karena ini pertama kalinya mereka benar-benar "belum memiliki koneksi dunia nyata" dan "hanya akun Twitter" untuk membuktikan keterlibatan dalam kasus teror. Misalnya, Mehdi, meskipun "dukungan ideologisnya yang terbuka" bukanlah "anggota terdaftar atau terdaftar dari IS", juga tidak ada bukti untuk membuktikan bahwa "dia mengambil arah atau terlibat dalam aktivitas dunia nyata lainnya untuk IS" . Dia adalah "penjaga hutan yang lebih lama" dan cukup banyak beroperasi sendiri dan sejauh ini tidak ada bukti untuk membuktikan bahwa keterlibatannya di luar tweetnya, tambahnya. Tapi kemudian, ada ribuan "penjaga tunggal" di dunia maya yang mengklaim mewakili ratusan ideologi "kelinci dan teroris" dan karenanya pertanyaannya - berapa banyak bukti yang dapat dimiliki oleh tweet saja dalam kasus seperti ini?

Seorang pengacara berbasis di Mumbai yang mengkhususkan diri dalam hukum cyber, Pawan Duggal, mengatakan bahwa kasus ini bukan hanya tentang tweet dan terorisme, tetapi tentang hukum cyber India dan kemampuan mereka untuk menangani insiden tersebut. “Di bawah bahasa Bagian 66 F Undang-Undang Teknologi Informasi, tweet saja tidak memenuhi parameter terorisme Cyber” dan ini hanya menunjukkan “kebutuhan untuk meninjau kembali undang-undang untuk mendefinisikan dan memfokuskan penggunaan media sosial untuk cyber terorisme,” bantahnya. Mr. Duggal menambahkan bahwa “undang-undang tersebut diamandemen pada tahun 2008 dan sejak itu banyak yang berubah dalam hal teknologi dan ini hanya menunjukkan bahwa undang-undang dunia maya perlu mengikuti perubahan teknologi yang cepat” dan bahwa ada “kebutuhan mendesak untuk fokus pada internet seluler dan sosial penyalahgunaan media untuk mendefinisikan kembali teror dunia maya, perang atau naxalisme.”

Namun, di latar belakang saat ini, kuncinya di depan penyidik adalah untuk membuktikan "hubungan dunia nyata". Penyelidik mengatakan bahwa setidaknya, mereka dapat mendakwa Mehdi karena Menjadi 'propagandis' untuk ISIS, melanjutkan perjuangan mereka untuk mengobarkan perang melawan rezim di Suriah dan Irak. "Kami memiliki bukti, beberapa bahkan melalui tweet publik oleh pejuang ISIS bahwa dia adalah agen radikal dan motivator, yang bersekongkol dengan Kejahatan," kata seorang pejabat. Polisi juga mengandalkan 14.000 plus pesan langsung pribadi di Twitter untuk membuktikan bahwa dia menghasut orang-orang untuk memperjuangkan IS, yang mereka klaim cukup untuk mendakwanya berdasarkan Bagian 39 UAPA, 2004 dan Bagian 125 IPC karena mendukung teror. pakaian dan bersekongkol untuk mengobarkan perang melawan sekutu Asia yang Ramah. Sementara ISIS sendiri tidak dinyatakan sebagai “kelompok terlarang” di bawah

hukum India pada saat penangkapan Mehdi, para penyelidik berpendapat bahwa ISIS dinyatakan sebagai “kelompok teroris” oleh PBB dan telah melakukan “tindakan teror ekstrem.” Ini secara otomatis berarti bahwa dukungan untuk itu dapat ditafsirkan sebagai “aksi teror” di bawah UAPA, bantah mereka.

Namun, pengacara yang berbasis di Bengaluru, Jaffer Shah, yang akan mewakili Mehdi dalam kasus ini, mengatakan bahwa kasus ini menimbulkan "pertanyaan mendasar" tentang apakah pengungkapan "pendapat dan dukungan ideologis dan informasi retweet atau tweeting" dapat dianggap sebagai kasus penipuan. perang melawan sekutu Asia yang bersahabat, yang merupakan terorisme dunia maya di bawah Undang-Undang TI. Mr Shah lebih lanjut berpendapat bahwa kasus ini akan menentukan "di mana kita kemudian menarik perbedaan antara ribuan tweet kebencian atau perang yang dikeluarkan dan tindakan teror". "Polisi tampaknya telah menyatakan bahwa ekspresi dukungan ideologis dan pendapat yang mendukung IS adalah tindakan teror, pembelaan kami adalah mempertanyakan premis itu," tambahnya.

Dalam konteks ini, beberapa putusan Mahkamah Agung dikutip oleh para ahli hukum, termasuk perintah 2007 dalam kasus Arup Bhuyan vs. Negara Bagian Assam, di mana dua hakim memutuskan bahwa bahkan “keanggotaan organisasi terlarang saja tidak akan membuat seseorang menjadi kriminal kecuali dia menggunakan kekerasan atau menghasut orang untuk melakukan Kekerasan atau menciptakan kekacauan publik dengan kekerasan atau hasutan untuk melakukan kekerasan. “Pengacara hak asasi manusia terkemuka Anand Grover mengatakan: “Kecuali ada keterlibatan langsung dalam suatu tindakan, sulit untuk membuktikan kasus-kasus ini” dan mereka termasuk dalam “wilayah abu-abu”.

Menurut pengakuan Mehdi sendiri kepada para interogator, dia “tidak tertarik untuk menciptakan gerakan di tanah India” dan kasus yang menentangnya adalah dalam konteks “sekutu Asia yang bersahabat.” Mr. grover menunjukkan bahwa kasus-kasus seperti itu adalah "pertanyaan terbuka yang ditentukan oleh konteks politik" tentang apa yang merupakan "tindakan terorisme" dan apa yang tidak.

Dengan ukuran apa pun, ini adalah kasus kompleks yang muncul di sekitar seorang pria, yang melalui beberapa ribu tweet, telah menyatakan dan menyatakan dukungan untuk gerakan "teroris" yang kejam. Sementara bukti terhadap Mehdi akan menjadi kunci bagi para penyelidik, kasus itu sendiri dapat memiliki konsekuensi yang jauh lebih besar dalam mendefinisikan penggunaan atau penyalahgunaan media sosial: itu dapat mendefinisikan kembali seberapa jauh sebuah tweet dapat digunakan dalam “perang melawan Negara mana pun”.

15.6 STUDI KASUS-II

India harus bangun dari terorisme dunia maya' (Haris Zargar, Layanan Berita Indo-Asian, 02 April 2013): Pada awal Maret, para peretas China yang dicurigai melanggar komputer organisasi militer top India, Organisasi Penelitian dan Pengembangan Pertahanan (DRDO) , dalam apa yang disebut-sebut sebagai salah satu pelanggaran keamanan terbesar dalam sejarah negara itu. Mantan Menteri Pertahanan A.K. Antony memerintahkan penyelidikan atas masalah ini, meskipun pernyataan resmi membantah file sensitif telah dikompromikan. India telah menyaksikan banyak serangan semacam itu terhadap instalasi kritisnya dan

penyalahgunaan media sosial dan Internet telah membawa pulang ancaman terorisme siber, yang menurut pakar keamanan siber negara itu tidak siap untuk ditangani. Para ahli percaya negara itu rentan terhadap serangan terorisme dunia maya seperti itu dengan beberapa negara dan kelompok-kelompok kepentingan yang cenderung melakukan spionase dan perusakan.

Menurut pengacara Mahkamah Agung dan pakar hukum siber terkemuka Pavan Duggal, sementara ancaman serangan siber tetap "sudah dekat", negara itu tidak memiliki mekanisme pasukan siber yang dilembagakan untuk menangani ancaman tersebut. “Pelanggaran DRDO baru-baru ini adalah kasus klasik serangan perang siber dan bukan sekadar peretasan. Itu adalah serangan terhadap infrastruktur informasi penting India. Perang siber sebagai fenomena tidak tercakup dalam undang-undang siber India. Jelas, keamanan siber negara tidak selaras dengan tuntutan zaman," kata Duggal kepada IANS.

Selama beberapa tahun terakhir, India telah menyaksikan semakin banyak serangan dunia maya, dengan departemen pemerintah, terutama lembaga pertahanan, diserang. Tahun lalu, kelompok peretas 'Anonymous' melakukan serangkaian serangan Distributed Denial of Service (DDoS) terhadap sejumlah situs web pemerintah, sebagai pembalasan terhadap dugaan sensor internet. Peretas dari Aljazair juga melakukan serangan terhadap situs web yang dijalankan oleh DRDO, Kantor Perdana Menteri dan berbagai departemen pemerintah lainnya tahun lalu. Sebuah kelompok bernama 'Pakistan Cyber Army' juga telah meretas beberapa situs web India. "Lanskap ancaman tetap sangat mengancam," kata pakar hukum siber dan keamanan siber Prashant Mali. "India sadar akan ancaman global perang siber sekarang. Keamanan siber kita masih tidak efektif karena kebangkitan massal ke arah itu hilang atau tidak memadai. Meskipun NTRO dan DRDO diamanatkan dengan pekerjaan serangan siber, hanya waktu yang akan menunjukkan keefektifan organisasi-organisasi ini, " kata Mali kepada IANS.

Biasanya, serangan siber mengikuti modus operandi yang sama. Email dikirim ke individu atau grup kecil, di dalam organisasi. Upaya yang dilakukan untuk membuat email terlihat sah, yaitu, akan tampak seolah-olah dikirim oleh seseorang yang dipercaya oleh penerima dan isi email sering kali terkait dengan bidang minat penerima. Untuk menginstal malware, pengguna ditipu untuk mengklik tautan berbahaya atau meluncurkan lampiran berbahaya. Dalam serangan yang lebih canggih, penyerang akan menggunakan "kerentanan nol hari" baru, di mana penyerang mengirim lampiran email yang ketika dibuka, mengeksploitasi kerentanan di browser Web.

Menurut CERT-In (Tim Tanggap Darurat Komputer India), yang merupakan organisasi keamanan teknologi informasi yang dimandatkan pemerintah; diperkirakan 14.392 situs web di negara ini diretas pada tahun 2012 (hingga Oktober). Pada tahun 2011, sebanyak 14.232 diretas, sedangkan jumlah situs web yang diretas pada 2009 mencapai 9.180. Sekitar 16.126 situs web diretas pada tahun 2010. Dengan keamanan siber yang berdampak pada keamanan negara, Shivshankar Menon, penasihat keamanan nasional, mengumumkan bulan lalu bahwa pemerintah menerapkan arsitektur keamanan siber nasional untuk mencegah sabotase, spionase, dan bentuk ancaman dunia maya lainnya.

"Beberapa tahun terakhir telah menyaksikan perubahan dramatis dalam lanskap ancaman. Motivasi penyerang telah beralih dari ketenaran menjadi keuntungan finansial dan

malware telah menjadi model bisnis kriminal yang sukses dengan miliaran dolar dalam permainan. Kami sekarang telah memasuki perubahan signifikan ketiga dalam lanskap ancaman, salah satu spionase siber dan sabotase siber," Shantanu Ghosh, wakil presiden di India Product Operations-Symantec corporation, yang mengembangkan Norton AntiVirus, mengatakan kepada IANS. Ghosh mengatakan pertanyaan keamanan dunia maya tidak lagi menjadi topik eksotis yang berfokus terutama pada pesan spam dan komputer pribadi, tetapi telah mulai berdampak pada kemampuan keamanan dan pertahanan nasional suatu negara. Rikshit Tandon, konsultan di Internet and Mobile Association of India (IAMAI) dan penasihat Unit Kejahatan Siber Kepolisian Uttar Pradesh, mengatakan: "Terorisme siber adalah ancaman besar tidak hanya bagi India tetapi juga bagi dunia." "Itu bisa datang ke negara mana pun dan, ya, tindakan proaktif oleh pemerintah dan konsorsium negara perlu diambil sebagai upaya dan kebijakan kolektif karena internet tidak memiliki batas geografis," kata Tandon kepada IANS. Para ahli mengatakan negara itu menghabiskan sedikit uang untuk keamanan siber.

Alokasi anggaran untuk keamanan siber adalah Rs.42,2 crore (Rp 116.400juta) untuk 2012-13, dibandingkan Rs.35,45 crore pada tahun 2010- 11. Sebagai perbandingan, AS menghabiskan beberapa miliar dolar melalui National Security Agency, Rp 9.870.000 juta melalui Departemen Keamanan Dalam Negeri dan $93 juta melalui US-CERT pada 2013.

15.7 STUDI KASUS-III

Studi Kasus Ledakan Ahmadabad

Ahmadabad adalah jantung budaya dan komersial negara bagian Gujarat, dan salah satu kota terbesar di India. Pada tanggal 26 Juli 2008, serangkaian 21 ledakan bom menghantam Ahmedabad dalam rentang waktu 70 menit. 56 orang tewas dan lebih dari 200 orang terluka. Beberapa saluran TV menyatakan bahwa mereka telah menerima email dari kelompok teror bernama Mujahidin India yang mengaku bertanggung jawab atas serangan teror tersebut.

Fiist Mail dikirim pada 26 Juli 2008 dari email Id alarbi_gujarat@yahoo.com dari alamat IP 210.211.133.200 yang ditelusuri ke Rumah Kenneth Haywood di Navi Bombay. Router WIFI Tidak Aman miliknya disalahgunakan oleh teroris untuk mengirim surat teror dari routernya. Karena sistem log dinonaktifkan, Polisi tidak dapat mengetahui detail alamat MAC pelakunya. Surat kedua dikirim pada 31 Juli 2008 dari alarbi_gujarati@yahoo.com dari Alamat IP: 202.160.162.179 yang ditelusuri ke Medical College di Vaghodiya, Baroda, Gujarat. Agak sulit untuk melacak surat ini karena surat telah dikirim menggunakan server proxy & skrip surat palsu tetapi akhirnya Polisi dengan bantuan ahli Cyber melacak alamat IP asli.

Surat ketiga dikirim pada 23 Agustus 2008 dari alarbi.alhindi@gmail.com dari alamat IP: 121.243.206.151 yang ditelusuri ke Khalsa College di Bombay. Sekali lagi router WIFI tidak aman disalahgunakan untuk mengirim email. Dari Mail dikirim pada 13 September 2008 dari al_arbi_delhi@yahoo.com yang ditelusuri ke Kamran Power Limited di Bombay. Dalam hal ini juga router WIFI disalahgunakan untuk mengirim surat ancaman.

15.8 STUDI KASUS-IV

Studi Kasus Serangan 26/11

Mumbai adalah ibu kota negara bagian Maharashtra dan kota terbesar di India. Serangan dilakukan pada 26 November 2008 dan berlangsung hingga 29 November. Serangan terdiri dari lebih dari sepuluh penembakan dan pengeboman terkoordinasi. Seorang saksi FBI telah menyelidiki bahwa teroris berhubungan dengan penangan mereka di Pakistan melalui Callphonex menggunakan VOIP.

Terdakwa yang dicari dalam kasus serangan 26/11 telah berkomunikasi dengan teroris menggunakan ID email yang diakses dari sepuluh alamat IP -Lima dari Pakistan, dua Amerika Serikat, dua Rusia dan satu Kuwait. Kharak_telco@yahoo.com adalah ID email yang digunakan oleh tersangka buronan saat berkomunikasi dengan teroris melalui Voice over Internet Protocol (VoIP) melalui Callphonex yang berbasis di New Jersey. Menurut pemilik "callphonex" pada tanggal 20 Oktober, ia telah menerima email dari nama "Kharak Singh", menyatakan keinginan untuk membuka rekening dengan Callphonex.

Terdakwa telah menggunakan layanan Callphonex berikut:

- 15 panggilan dari komputer ke telepon,
- 10 panggilan ke akun klien umum dan
- Panggilan langsung ke dalam

Mereka telah mengakses ID email dari sepuluh alamat IP, lima di antaranya milik Pakistan. Salah satu alamat (118.107.140.138) dilacak ke Kolonel R Sadat Ullah dari Organisasi Komunikasi Khusus, Qasim Road, Rawalpindi, Pakistan. Tiga alamat dilacak ke Operasi jaringan Panggilan Dunia dan yang kelima berasal dari Sajid Iftikar, Rumah EFU, Jalan Penjara di Pakistan. Lima alamat IP lainnya, dari mana alamat email kharak_telco@yahoo.com diakses, dilacak ke server FDC.net di Chicago (AS), Ahemed Mekky di Kuwait dan Vladimir N Zernov di Perusahaan Saham Gabungan, Moskow.

15.9 STUDI KASUS-V

2008: Tahun terorisme dunia maya: (Oleh Pavan Duggal 08 Jan 2009):

Tahun 2008 juga merupakan tahun di mana berbagai kejahatan dunia maya menjadi pusat perhatian. Berbagai kasus pencurian identitas dan phishing dilaporkan, meskipun angka yang dilaporkan jauh melampaui kasus yang dilaporkan. Di tengah semua ini, hukum siber India terus tampak ompong. Sementara itu, ketika internet 2.0 menjadi lebih menonjol di India, kejahatan dunia maya jejaring sosial, termasuk penyalahgunaan informasi pribadi yang diposting di situs semacam itu sering dilaporkan. Penyalahgunaan informasi pribadi dengan merusak dan mengubah hal yang sama, telah berkembang pesat. Tahun itu juga merupakan tahun terorisme dunia maya.

Apakah itu Bangalore atau Delhi, ledakan bom didahului oleh e-mail yang mengumumkan tindakan yang akan datang. Itu adalah tahun ketika teroris cyber menjadi jauh lebih berani. Ketidakmampuan lembaga penegak hukum untuk menangkap penjahat dunia maya dan mengambil tindakan yang efektif mengungkap kelemahan hukum kita. Terorisme dunia maya sekali lagi muncul di India dalam bentuk serangan Mumbai. Teroris sangat paham teknologi, dan menggunakan telepon satelit dengan impunitas. Itu adalah tahun, ketika didorong oleh serangan Mumbai, pemerintah bertindak dan mendapatkan amandemen Undang-Undang Teknologi Informasi, 2000 disahkan di kedua gedung Parlemen . Jelas, fakta

pengesahan Undang-Undang Amandemen Teknologi Informasi, 2008 di kedua majelis tanpa diskusi, menunjukkan kebenaran diktum bahwa sejarah berulang.

Pada tahun 2000, UU IT disahkan tanpa diskusi di kedua gedung DPR. Hal yang sama terulang di India pada Desember 2008. Akibatnya, alih-alih menangani terorisme dunia maya secara komprehensif, amandemen UU TI hanya memiliki satu ketentuan tentang terorisme dunia maya. Tampaknya tidak ada tanda-tanda pelajaran dari serangan Mumbai. Amandemen ini sekarang menunggu persetujuan Presiden. Itu adalah tahun di mana penyedia layanan jaringan mulai merasakan panasnya proses hukum. Berbagai litigasi diajukan menuntut mereka untuk mengungkapkan informasi pihak ketiga yang diberikan dan tersedia di sistem komputer mereka. Sebuah penyedia layanan jaringan merasakan akibat memberikan informasi pelanggan yang salah kepada penegak hukum.

Tahun membawa pulang kebenaran bahwa jika penyedia layanan jaringan lalai dalam memberikan informasi pelanggan yang benar kepada lembaga penegak hukum, mereka harus menghadapi konsekuensi hukum potensial, baik perdata maupun pidana. Terlebih lagi, karena di bawah Undang-Undang TI, 2000, penyedia ini bertanggung jawab atas semua data dan informasi pihak ketiga yang disediakan oleh mereka. Namun, mereka dapat keluar dari tanggung jawab mereka, asalkan mereka dapat membuktikan dua kondisi. Syarat pertama adalah penyedia layanan jaringan harus membuktikan bahwa ia tidak mengetahui adanya pelanggaran hukum. Kondisi kedua adalah bahwa penyedia harus membuktikan bahwa meskipun uji tuntas, hal itu tidak dapat mencegah dilakukannya suatu pelanggaran atau pelanggaran hukum.

Pada tahun 2008, India menyelenggarakan acara internasional besar yang berkaitan dengan IT dan internet. Pada bulan Februari 2008, pertemuan Delhi dari Internet Corporation For Assigned Names And Numbers (Icann) diadakan. Menjelang akhir Desember 2008, pemerintah menyelenggarakan Forum Tata Kelola Internet di Hyderabad. Forum ini sangat penting dalam hal memberikan platform bersama kepada semua pemangku kepentingan internet untuk membahas isu-isu yang berkaitan dengan hukum dan kebijakan internet. Itu juga merupakan tahun penting untuk penilaian yang diberikan di bawah Undang-Undang Teknologi Informasi. 2000. Pada bulan Februari 2008, L Prakash, seorang ahli bedah ortopedi, dijatuhi hukuman seumur hidup atas tuduhan cabul online.

Pada bulan Mei, Pengadilan Tinggi Delhi memberikan keputusan penting dalam kasus Baazee.com. CEO portal ditangkap pada tahun 2004 karena menghosting pesan yang berkaitan dengan DPS MMS di situs webnya. Dalam hal ini, pemerintah memungut tuntutan pidana dan mengajukan surat dakwaan. Ini ditantang di depan Pengadilan Tinggi Delhi, yang menolak untuk membatalkan tuduhan kriminal dunia maya atas kecabulan online dan mengarahkan terdakwa untuk menghadapi persidangan pidana. Kasus tersebut kini sedang diproses di Mahkamah Agung. Hasil umum dari putusan ini adalah bahwa prinsip-prinsip hukum untuk informasi elektronik, sebagaimana diatur dalam Undang-undang, telah ditegakkan. Tahun 2008 adalah tahun yang penuh petualangan sejauh menyangkut yurisprudensi hukum siber di India. Perkembangan hukum siber yang terjadi akan memberikan landasan bagi pertumbuhan dan perkembangan selanjutnya dari yurisprudensi hukum siber India di tahun 2009. Akan menarik untuk melihat bagaimana tahun ini menghadapi tantangan yang berkaitan dengan internet, ruang siber dan world wide web.

15.10 RINGKASAN

Konsep terorisme dunia maya dalam perspektif India juga merupakan aspek yang sangat penting. Dalam unit ini berbagai konsep penting tentang terorisme siber-makna dan definisi dalam perspektif India menurut hukum India, terorisme siber di bawah Undang-Undang Teknologi Informasi, 2000, terorisme siber dan KUHP India, 1860, terorisme siber di India dan solusinya dalam situasi sekarang. dan studi kasus dibahas untuk dipahami demi kepentingan siswa.

15.11 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Authorpress)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang tepat dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

15.12 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Ancaman yang ditimbulkan oleh terorisme siber telah menarik perhatian media massa, komunitas keamanan, dan industri TI.
b) Ungkapan "terorisme dunia maya" mencakup penggunaan teknologi informasi yang bersifat negatif dan berbahaya secara internasional.
c) Undang-undang yang menangani terorisme dunia maya, bagaimanapun, tidak cukup untuk memenuhi niat berbahaya dari teroris dunia maya ini.
d) Terorisme dunia maya mencakup upaya untuk menembus atau mengakses sumber daya komputer tanpa izin.
e) Kepala NASSCOM mengatakan perusahaan India rata-rata hanya menghabiskan 0,8 persen dari anggaran teknologi mereka untuk keamanan, dibandingkan rata-rata global 5,5%.

B. Isi Bagian yang Kosong:

I. …….. Dari Undang-Undang Teknologi Informasi tahun 2000 terkait dengan cyber terrorism.
II. bagian mendefinisikan …… seperti, penolakan akses tidak sah atau serangan layanan, dll.
III. Ancaman terorisme dunia maya bukan hanya tanggung jawab ……..
IV. Sebuah …… undang-undang selalu merupakan langkah maju yang baik untuk memerangi terorisme dunia maya.
V. Barang siapa melakukan atau berkompromi untuk melakukan terorisme siber dipidana dengan pidana penjara yang …….

15.13 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Bagian 66F
2. Serangan siber konvensional
3. Negara dan Perangkatnya
4. Tepat waktu dan tepat
5. Dapat diperpanjang hingga penjara seumur hidup

15.14 PERTANYAAN TERMINAL

1. Apa arti dan definisi terorisme dunia maya dalam perspektif India?
2. Membahas terorisme dunia maya berdasarkan UU IT, 2000.
3. Membahas terorisme dunia maya dan KUHP India, 1860.
4. Diskusikan Studi Kasus-I dan II.
5. Diskusikan studi kasus-III dan IV.

BAB 16
TERORISME CYBER DAN HAK ASASI MANUSIA

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu dan pokok bahasan yang terkait dengan Cyber Terrorism dan Hak Asasi Manusia
- Memahami pentingnya Hak Asasi Manusia dengan mengacu pada Terorisme Cyber
- Memahami masalah teknis dan hukum terkait Cyber Terrorism dengan mengacu pada Cyber Terrorism

16.1 PENGANTAR

Isu terorisme dan hak asasi manusia telah lama menjadi perhatian PBB. Menyusul serangan teroris 11 September 2001 dan lonjakan aksi terorisme di seluruh dunia, hal itu menjadi semakin mendesak. Sementara mengutuk terorisme dengan tegas dan mengakui tugas Negara untuk melindungi mereka yang tinggal di dalam yurisdiksi mereka dari terorisme, PBB telah menempatkan prioritas pada pertanyaan untuk melindungi hak asasi manusia dalam konteks tindakan kontra-terorisme. Pembelaan hak asasi manusia dan penegakan supremasi hukum saat melawan terorisme memang merupakan inti dari Strategi Kontra-Terorisme Global Perserikatan Bangsa-Bangsa. Negara-negara Anggota mengakui bahwa tindakan kontra-terorisme yang efektif dan perlindungan hak asasi manusia bukanlah tujuan yang saling bertentangan tetapi tujuan yang saling melengkapi dan memperkuat. Mereka berjanji untuk mengambil langkah-langkah yang ditujukan untuk menangani pelanggaran hak asasi manusia dan untuk memastikan bahwa setiap tindakan yang diambil untuk melawan terorisme mematuhi kewajiban hak asasi manusia mereka.

Dukungan konkrit oleh Negara-negara Anggota tentang perlunya menjadikan perlindungan hak asasi manusia sebagai bagian integral dari perang internasional melawan terorisme ditunjukkan dengan dibentuknya jabatan Pelapor Khusus pada tahun 2005 tentang pemajuan dan perlindungan hak asasi manusia dan kebebasan fundamental sementara melawan terorisme. Pelapor Khusus, yang beroperasi di bawah Dewan Hak Asasi Manusia yang baru, bekerja untuk mengidentifikasi, bertukar, dan mempromosikan praktik-praktik terbaik tentang langkah-langkah untuk melawan terorisme yang menghormati hak asasi manusia dan kebebasan mendasar. Pelapor Khusus juga membahas tuduhan pelanggaran hak asasi manusia dalam rangka melawan terorisme. Dia melakukan kunjungan ke negara-negara tertentu dan telah terlibat dalam korespondensi dengan lebih dari 40 negara tentang hukum dan praktik mereka. Dia melaporkan secara teratur baik kepada Dewan Hak Asasi Manusia dan Majelis Umum, termasuk pada isu-isu tematik yang dipilih dan kunjungan negaranya.

16.2 KONVENSI INTERNASIONAL TENTANG TERORISME-I

Ringkasan 14 instrumen hukum utama dan amandemen tambahan yang berhubungan dengan terorisme:

1. Konvensi 1963 tentang Pelanggaran dan Tindakan Tertentu Lainnya yang Dilakukan Di Pesawat Terbang (Konvensi Pesawat):
   - Berlaku untuk tindakan yang mempengaruhi keselamatan dalam penerbangan;
   - Memberi wewenang kepada komandan pesawat untuk menerapkan tindakan yang wajar, termasuk menahan diri, pada setiap orang yang dia yakini telah atau akan melakukan tindakan tersebut, jika perlu untuk melindungi keselamatan pesawat; dan
   - Mengharuskan Negara-negara yang mengadakan kontrak untuk menahan para pelanggar dan mengembalikan kendali pesawat kepada komandan yang sah.
2. Konvensi 1970 untuk Pemberantasan Perampasan Pesawat Udara yang Tidak Sah (Unlawful Seizure Convention):
   - Menjadikan pelanggaran bagi setiap orang yang berada di dalam pesawat dalam penerbangan untuk "secara melawan hukum, dengan kekerasan atau ancamannya, atau bentuk intimidasi lainnya, [untuk] merebut atau mengendalikan pesawat itu" atau mencoba melakukannya;
   - Mengharuskan pihak-pihak dalam konvensi untuk membuat pembajakan dapat dihukum dengan "hukuman berat"
   - Mengharuskan pihak yang memiliki hak asuh pelaku untuk mengekstradisi pelaku atau menyerahkan kasus untuk penuntutan; dan
   - Mengharuskan para pihak untuk saling membantu sehubungan dengan proses pidana yang dibawa di bawah Konvensi.
   - Protokol Tambahan 2010 untuk Konvensi Penindasan Perampasan Pesawat Secara Tidak Sah
   - Melengkapi Konvensi untuk Pemberantasan Perampasan Pesawat yang Tidak Sah dengan memperluas cakupannya untuk mencakup berbagai bentuk pembajakan pesawat, termasuk melalui sarana teknologi modern;
   - Menggabungkan ketentuan Konvensi Beijing yang berkaitan dengan ancaman atau konspirasi untuk melakukan pelanggaran.
3. Konvensi 1971 untuk Pemberantasan Perbuatan Melanggar Hukum terhadap Keselamatan Penerbangan Sipil (Konvensi Penerbangan Sipil):
   - Menjadikan suatu pelanggaran bagi setiap orang yang secara melawan hukum dan dengan sengaja melakukan tindakan kekerasan terhadap seseorang di dalam pesawat udara dalam penerbangan, jika tindakan tersebut dapat membahayakan keselamatan pesawat udara; menempatkan alat peledak di pesawat terbang; untuk mencoba tindakan tersebut; atau menjadi kaki tangan dari orang yang melakukan atau mencoba melakukan tindakan tersebut;
   - Mengharuskan para pihak Konvensi untuk membuat pelanggaran dihukum dengan "hukuman berat"; dan
   - Mengharuskan pihak-pihak yang memiliki hak asuh atas pelaku untuk mengekstradisi pelaku atau menyerahkan kasus tersebut untuk penuntutan.
4. Konvensi 1973 tentang Pencegahan dan Penghukuman Kejahatan Terhadap Orang-Orang yang Dilindungi Secara Internasional (Konvensi Agen Diplomatik):
   - Mendefinisikan "orang yang dilindungi secara internasional" sebagai Kepala Negara, Menteri Luar Negeri, perwakilan atau pejabat suatu Negara atau organisasi

internasional yang berhak atas perlindungan khusus di suatu Negara asing, dan keluarganya; dan

- Mengharuskan pihak-pihak untuk mengkriminalisasi dan menghukum "dengan hukuman yang pantas yang memperhitungkan sifat serius mereka" pembunuhan yang disengaja, penculikan atau serangan lain terhadap orang atau kebebasan orang yang dilindungi secara internasional, serangan kekerasan terhadap tempat resmi, akomodasi pribadi , atau alat transportasi orang tersebut; ancaman atau upaya untuk melakukan serangan semacam itu; dan tindakan "merupakan partisipasi sebagai kaki tangan".

5. Konvensi Internasional 1979 Menentang Penyanderaan (Konvensi Penyanderaan):
   - Menetapkan bahwa "setiap orang yang menangkap atau menahan dan mengancam untuk membunuh, melukai, atau terus menahan orang lain untuk memaksa pihak ketiga, yaitu, suatu Negara, organisasi antar pemerintah internasional, orang perseorangan atau badan hukum, atau sekelompok orang, untuk melakukan atau tidak melakukan tindakan apapun sebagai syarat eksplisit atau implisit untuk pembebasan sandera, melakukan pelanggaran penyanderaan dalam pengertian Konvensi ini".
6. Konvensi 1980 tentang Perlindungan Fisik Bahan Nuklir (Konvensi Bahan Nuklir):
   - Mengkriminalisasi kepemilikan, penggunaan, pemindahan atau pencurian bahan nuklir secara tidak sah dan ancaman penggunaan bahan nuklir untuk menyebabkan kematian, cedera serius, atau kerusakan properti yang substansial.
   - Amandemen Konvensi tentang Perlindungan Fisik Bahan Nuklir
   - Membuatnya mengikat secara hukum bagi Negara-negara Pihak untuk melindungi fasilitas dan bahan nuklir dalam penggunaan, penyimpanan dan transportasi domestik yang damai; dan
   - Menyediakan kerjasama yang diperluas antara dan di antara Negara-negara mengenai langkah-langkah cepat untuk menemukan dan memulihkan bahan nuklir yang dicuri atau diselundupkan, mengurangi konsekuensi radiologis atau sabotase, dan mencegah dan memerangi pelanggaran terkait.
7. 1988 Protokol untuk Penindasan Tindakan Melanggar Hukum di Bandara yang Melayani Penerbangan Sipil Internasional, tambahan dari Konvensi untuk Penindasan Tindakan Melanggar Hukum terhadap Keselamatan Penerbangan Sipil (Memperluas dan melengkapi Konvensi Montreal tentang Keselamatan Udara) (Protokol Bandara) :
   - Memperluas ketentuan Konvensi Montreal untuk mencakup tindakan teroris di bandara yang melayani penerbangan sipil internasional.

16.3 KONVENSI INTERNASIONAL TENTANG TERORISME-II

8. Konvensi 1988 untuk Penindasan Tindakan Melanggar Hukum terhadap Keselamatan Navigasi Maritim (Konvensi Maritim):
   - Menetapkan rezim hukum yang berlaku untuk tindakan melawan navigasi maritim internasional yang serupa dengan rezim yang ditetapkan untuk penerbangan internasional; dan
   - Menjadikan pelanggaran bagi seseorang secara melawan hukum dan dengan sengaja untuk merebut atau melakukan kontrol atas kapal dengan kekerasan, ancaman, atau

intimidasi; melakukan tindakan kekerasan terhadap seseorang di atas kapal jika tindakan tersebut dapat membahayakan keselamatan navigasi kapal; menempatkan alat atau bahan perusak di atas kapal; dan tindakan lain yang bertentangan dengan keselamatan kapal.

- Protokol 2005 untuk Konvensi Pemberantasan Tindakan Melanggar Hukum terhadap Keselamatan Navigasi Maritim
- Mengkriminalisasi penggunaan kapal sebagai alat untuk melanjutkan aksi terorisme;
- Mengkriminalisasi pengangkutan di atas kapal berbagai bahan yang diketahui bahwa bahan tersebut dimaksudkan untuk digunakan untuk menyebabkan, atau dalam ancaman menyebabkan, kematian atau cedera serius atau kerusakan untuk melanjutkan tindakan terorisme;
- Mengkriminalisasi pengangkutan di atas kapal orang yang telah melakukan tindakan terorisme; dan
- Memperkenalkan prosedur untuk mengatur naik ke kapal yang diyakini telah melakukan pelanggaran menurut Konvensi.

9. 1988 Protokol untuk Pemberantasan Tindakan Melanggar Hukum Terhadap Keamanan Anjungan Tetap yang Berada di Landas Kontinen (Protokol Anjungan Tetap):
    - Menetapkan rezim hukum yang berlaku untuk tindakan terhadap platform tetap di landas kontinen yang serupa dengan rezim yang ditetapkan terhadap penerbangan internasional.
    - Protokol 2005 tentang Protokol untuk Pemberantasan Tindakan Melanggar Hukum terhadap Keamanan Platform Tetap yang Terletak di Landas Kontinen
    - Menyesuaikan perubahan Konvensi untuk Penindasan Tindakan Melanggar Hukum terhadap Keselamatan Navigasi Maritim dengan konteks platform tetap yang terletak di landas kontinen.
10. Konvensi 1991 tentang Penandaan Bahan Peledak Plastik untuk Tujuan Deteksi (Konvensi Bahan Peledak Plastik):
    - Dirancang untuk mengontrol dan membatasi penggunaan bahan peledak plastik yang tidak bertanda dan tidak terdeteksi (dinegosiasikan setelah pengeboman Pan Am penerbangan 103 1988);
    - para pihak diwajibkan di wilayah masing-masing untuk memastikan kontrol yang efektif atas bahan peledak plastik "tidak bertanda", yaitu yang tidak mengandung salah satu agen pendeteksi yang dijelaskan dalam Lampiran Teknis pada perjanjian;
    - Secara umum, setiap pihak harus, antara lain, mengambil tindakan yang diperlukan dan efektif untuk melarang dan mencegah pembuatan bahan peledak plastik yang tidak bertanda; mencegah pergerakan bahan peledak plastik yang tidak bertanda ke dalam atau ke luar wilayahnya; melakukan kontrol yang ketat dan efektif atas kepemilikan dan pemindahan bahan peledak tidak bertanda yang dibuat atau diimpor sebelum berlakunya Konvensi; memastikan bahwa semua persediaan bahan peledak tidak bertanda yang tidak dimiliki oleh militer atau polisi dihancurkan, dikonsumsi, ditandai, atau menjadi tidak efektif secara permanen dalam waktu tiga tahun; mengambil langkah-langkah yang diperlukan untuk memastikan bahwa bahan peledak plastik tak bertanda yang dipegang oleh militer atau polisi dihancurkan, dikonsumsi,

diberi tanda atau dibuat tidak efektif secara permanen dalam waktu lima belas tahun; dan, memastikan pemusnahan, sesegera mungkin, setiap bahan peledak tak bertanda yang diproduksi setelah tanggal berlakunya Konvensi untuk Negara tersebut.

11. Konvensi Internasional 1997 untuk Pemberantasan Bom Teroris (Konvensi Pengeboman Teroris):
    - Menciptakan rezim yurisdiksi universal atas penggunaan bahan peledak dan perangkat mematikan lainnya yang melanggar hukum dan disengaja di, ke dalam, atau terhadap berbagai tempat umum yang ditentukan dengan maksud untuk membunuh atau menyebabkan cedera tubuh yang serius, atau dengan maksud untuk menyebabkan perusakan besar-besaran di tempat umum .
12. Konvensi Internasional 1999 untuk Pemberantasan Pendanaan Terorisme (Konvensi Pendanaan Terorisme):
    - Mengharuskan pihak-pihak untuk mengambil langkah-langkah untuk mencegah dan menangkal pendanaan teroris, baik langsung maupun tidak langsung, melalui kelompok yang mengaku memiliki tujuan amal, sosial atau budaya atau yang juga terlibat dalam kegiatan terlarang seperti perdagangan narkoba atau penggunaan senjata;
    - Mengharuskan Negara untuk menahan mereka yang mendanai terorisme secara pidana, perdata atau administratif bertanggung jawab atas tindakan tersebut; dan
    - Menyediakan identifikasi, pembekuan, dan penyitaan dana yang dialokasikan untuk kegiatan teroris, serta pembagian dana yang dibatalkan dengan Negara lain berdasarkan kasus per kasus. Rahasia bank tidak lagi menjadi pembenaran yang memadai untuk menolak bekerja sama.
13. Konvensi Internasional 2005 untuk Pemberantasan Tindak Terorisme Nuklir (Konvensi Terorisme Nuklir):
    - Mencakup berbagai tindakan dan kemungkinan target, termasuk pembangkit listrik tenaga nuklir dan reaktor nuklir;
    - Meliputi ancaman dan upaya untuk melakukan kejahatan tersebut atau untuk berpartisipasi di dalamnya, sebagai kaki tangan;
    - Menetapkan bahwa para pelanggar harus diekstradisi atau dituntut;
    - Mendorong Negara-negara untuk bekerja sama dalam mencegah serangan teroris dengan berbagi informasi dan saling membantu sehubungan dengan penyelidikan kriminal dan proses ekstradisi; dan
    - Menangani situasi krisis (membantu Negara untuk memecahkan situasi) dan situasi pasca krisis (membuat bahan nuklir aman melalui Badan Tenaga Atom Internasional (IAEA).
14. Konvensi 2010 tentang Pemberantasan Perbuatan Melanggar Hukum Terkait Penerbangan Sipil Internasional (Konvensi penerbangan sipil baru):
    - Mengkriminalisasi tindakan menggunakan pesawat udara sipil sebagai senjata untuk menyebabkan kematian, cedera atau kerusakan;
    - Mengkriminalisasi tindakan menggunakan pesawat udara sipil untuk melepaskan senjata biologi, kimia dan nuklir (BCN) atau bahan serupa untuk menyebabkan

kematian, cedera atau kerusakan, atau tindakan penggunaan bahan tersebut untuk menyerang pesawat udara sipil;

- Mengkriminalisasi tindakan pengangkutan senjata BCN secara tidak sah atau materi terkait tertentu;
- Serangan siber terhadap fasilitas navigasi udara merupakan pelanggaran;
- Ancaman untuk melakukan pelanggaran dapat menjadi pelanggaran dengan sendirinya, jika ancaman tersebut dapat dipercaya.
- Konspirasi untuk melakukan pelanggaran, atau persamaannya, dapat dihukum.

16.4 TERORISME CYBER DAN HAK ATAS PRIVASI

Hukum privasi adalah pengakuan atas hak individu untuk dibiarkan sendiri dan agar ruang pribadinya tidak dilanggar. Hak atas privasi sebagai konsep yang independen dan khas berasal dari bidang hukum Tort. Namun belakangan ini, hak ini telah memperoleh status konstitusional [Rajagopal Vs Negara Bagian TN [(1994) 6 SCC 632], pelanggarannya menimbulkan konsekuensi perdata maupun pidana di bawah undang-undang masing-masing. Perusahaan dan penemuan modern telah, melalui invasi terhadap privasinya, membuatnya menderita sakit dan tekanan mental, jauh lebih besar daripada yang dapat ditimbulkan oleh cedera tubuh belaka. Hak atas privasi adalah bagian dari hak untuk hidup dan kebebasan pribadi yang diabadikan dalam Pasal 21 Konstitusi India. Dengan munculnya teknologi informasi, konsep tradisional tentang hak atas privasi telah mengambil dimensi baru, yang memerlukan pandangan hukum yang berbeda. Untuk menjawab tantangan ini dapat ditempuh jalan Undang-Undang Teknologi Informasi tahun 2000.

Berbagai ketentuan Undang-undang melindungi hak privasi online pengguna internet. Hak-hak ini tersedia untuk individu pribadi maupun terhadap teroris dunia maya. Bagian 1 (2) yang dibaca dengan Pasal 75 Undang-undang mengatur penerapan ekstra-teritorial dari ketentuan Undang-undang. Jadi, jika seseorang (termasuk warga negara asing) melanggar privasi seseorang melalui komputer, sistem komputer atau jaringan komputer yang berlokasi di India, dia akan bertanggung jawab berdasarkan ketentuan Undang-undang. Ini memperjelas bahwa yurisdiksi lengan panjang sama-sama tersedia terhadap teroris dunia maya, yang tindakannya telah mengakibatkan kerusakan properti, baik berwujud maupun tidak berwujud.

16.5 HAK ASASI MANUSIA DAN DEKLARASI UNIVERSAL HAK ASASI MANUSIA

Deklarasi Universal Hak Asasi Manusia dalam Pembukaannya berbicara tentang “kebebasan dari ketakutan dan keinginan”. Kebebasan dari rasa takut sebagian besar merupakan istilah yang bersifat psikologis, namun digunakan sangat luas saat ini terutama dalam kasus terorisme. Pasal 3 dari deklarasi tersebut mengatur hak atas "keamanan pribadi". Sebagaimana kita ketahui, istilah “orang” juga mencakup lingkungan tempat ia berada, berbeda dengan istilah “individu” yang dalam salah satu konsepnya membayangkannya sebagai sesuatu yang abstrak, terlepas dari kondisi-kondisi lain di sekitarnya. Jadi melindungi keamanan pribadi juga berarti melindungi koneksi sosial, ekonomi dan lainnya, "utas" yang terjalin dengan lingkungan. Selama dalam realitas modern ini kadang-kadang sebagian besar

didasarkan pada teknologi, komputer atau internet, perlindungan terorisme siber juga berkaitan dengan “keamanan orang”.

Pasal 5 dengan perlindungannya terhadap “perlakuan yang merendahkan”. Kerugian pribadi juga merupakan bagian dari degradasi dan memperlakukan seseorang dengan cara saat ini adalah sesuatu yang mungkin diberikan oleh tindakan kejahatan dunia maya seperti yang telah dibuktikan di atas. Salah satu ketentuan penting yaitu pasal 12 deklarasi. Ini menyatakan: "tidak seorang pun boleh diganggu secara sewenang-wenang dengan privasinya, atau serangan terhadap kehormatan atau reputasinya". "privasi" didefinisikan sebagai "kualitas atau keadaan terpisah dari perusahaan atau pengamatan" yang dikombinasikan dengan definisi lain "kebebasan dari gangguan yang tidak sah" yang diberikan oleh sumber yang sama, juga mencakup privasi data yang disimpan di komputer dan hak untuk nikmati keadaan pribadi tanpa campur tangan tanpa kehendak pribadi pemiliknya.

Pasal 17 mengatur hak atas properti dan pembatasan untuk merampas milik siapa pun yang memiliki. Properti didefinisikan sebagai "segala sesuatu yang dimiliki oleh seseorang atau badan", termasuk dua jenisnya: "properti nyata" dan "properti pribadi". Harta pribadi atau “kepribadian” termasuk “harta bergerak yang bukan merupakan harta benda, uang, atau investasi.

Pasal 19, bagaimanapun, memainkan peran yang berbeda dalam topik ini dan sebagian besar terkait dengan penggunaan internet oleh teroris pada umumnya.

16.6 HAK ASASI MANUSIA, PERSERIKATAN BANGSA-BANGSA DAN DUNIA CYBER

Perlindungan Hak Asasi Manusia di Dunia Maya sangat dibutuhkan di tingkat Nasional dan Internasional. Seruan bagi PBB untuk mengambil ini adalah 'Lambat' ih nbim hal. Tidak ada waktu dalam sejarah Internet dan Cyberspace kebutuhan akan Perlindungan Hak Asasi Manusia di Cyberspace lebih dari saat ini. Jika PBB percaya pada Hak Asasi Manusia, ia harus mulai berpikir ke arah bentuk barunya di Era Internet ini. Tidak ada alasan mengapa Hak Asasi Manusia di Dunia Maya harus diberikan kepentingan yang lebih rendah daripada Hak Asasi Manusia tradisionalnya. Lagi pula Hak Asasi Manusia seperti Hak Berbicara dan Berekspresi, Hak atas Informasi, Hak untuk Tahu, Hak Privasi, dll serupa di Cyberspace. Justru pelanggaran HAM di dunia maya jauh lebih mudah dan sering terjadi. Yang paling mengejutkan adalah mengapa PBB masih belum menganggap Cyberspace sebagai bagian penting dari kehidupan manusia.

Jika kita menganalisis tren di seluruh dunia, teknologi semakin banyak digunakan untuk melanggar Hak Asasi Manusia di dunia maya. Oleh karena itu, PBB harus segera melindungi HAM di dunia maya. Bahkan komunitas Dunia Hak Asasi Manusia, Hukum Siber dan Keamanan Siber harus mulai berpikir ke arah ini karena isu-isu seperti Perang Siber, Terorisme Siber, Spionase Siber, Kejahatan Siber, Pengawasan Elektronik, Penyadapan Melanggar Hukum, dll bersifat “Transnasional”. Jika Negara yang berbeda akan memiliki undang-undang yang berbeda untuk masalah ini, akan sangat sulit untuk benar-benar menegakkan ketentuan perlindungan terhadap ancaman ini di tingkat Nasional dan Internasional. Inilah alasan mengapa kita harus “Harmonised Legal Framework” Dalam hal ini, sebaiknya di bawah rezim Organisasi Hak Asasi Manusia Perserikatan Bangsa-Bangsa.

Pemerintah di seluruh Dunia terlibat dalam penyadapan dan penyadapan telepon yang ilegal dan melanggar hukum. Hal ini melanggar berbagai Hak Asasi Manusia yang harus segera ditanggulangi oleh Masyarakat Internasional. Kerangka Kerja PBB untuk Hak Asasi Manusia saat ini dapat "Diubah dengan tepat" untuk mengakomodasi Hak Asasi Manusia di Dunia Maya. Hampir semua Negara di Dunia adalah Anggota PBB dan ini akan memperluas Perlindungan Hak Asasi Manusia di Dunia Maya kepada Warganya secara otomatis. Seruan itu harus diambil oleh PBB dan semakin cepat diambil, akan lebih baik bagi warga di seluruh dunia. Ambil contoh India. Hukum Cyber India melanggar berbagai Hak Asasi Manusia di Dunia Maya. Inilah alasan utama mengapa kami memulai Pusat Perlindungan Hak Asasi Manusia Cyberspace eksklusif di India. Begitu banyak ofensif adalah Hukum Cyber India yang layak untuk dicabut. Selanjutnya, Pemerintah India meluncurkan Proyek seperti Aadhar, National Intelligence Grid (NATGRID), Crime and Criminal Tracking Network and Systems (CCTNS), National Counter Terrorism Center (NCTC), Central Monitoring System (CMS), Center for Communication Security Research and Monitoring (CCSRM), dll. Tak satu pun dari mereka diatur oleh Kerangka Hukum apapun dan tidak satupun dari mereka berada di bawah Pengawasan Parlemen.

Jika tidak ada "Standar yang Dapat Diterima secara Internasional" untuk Perlindungan Hak Asasi Manusia di Dunia Maya, Negara-negara seperti India akan terus memberlakukan dan menerapkan Hukum Draconian seperti Undang-Undang Teknologi Informasi, 2000, Undang-Undang Telegraf India, 1885, Undang-Undang Rahasia Resmi, dll. Terakhir, PBB telah menunjukkan beberapa kecenderungan dalam hal ini. PBB sekarang menganggap akses Internet sebagai Hak Asasi Manusia dan menganggap pemutusan hubungan orang dari Internet sebagai pelanggaran Hak Asasi Manusia dan Hukum Internasional. Sebuah Laporan oleh Sidang ke-17 Dewan Hak Asasi Manusia PBB menggarisbawahi sifat "unik dan transformatif" dari internet yang memungkinkan individu untuk menjalankan berbagai Hak Asasi Manusia, dan untuk mempromosikan kemajuan masyarakat secara keseluruhan.

16.7 PEJUANG TERORIS ASING

Resolusi Dewan Keamanan PBB 2178 tentang Pejuang Teroris Asing-New York, NY-24 September 2014:

Resolusi 2178 mengharuskan negara-negara untuk mengambil langkah-langkah tertentu untuk mengatasi ancaman FTF, termasuk mencegah FTF yang dicurigai memasuki atau transit di wilayah mereka dan menerapkan undang-undang untuk menuntut FTF. Ia juga meminta negara-negara untuk melakukan berbagai langkah untuk meningkatkan kerja sama internasional di bidang ini, seperti dengan berbagi informasi tentang investigasi kriminal, larangan dan penuntutan. Dalam resolusi ini, untuk pertama kalinya, Dewan menggarisbawahi bahwa Countering Violent Extremism (CVE) adalah elemen penting dari respon yang efektif terhadap fenomena FTF. Resolusi 2178 juga memfokuskan badan kontraterorisme PBB yang ada pada ancaman FTF, menyediakan kerangka kerja untuk pemantauan dan bantuan jangka panjang kepada negara-negara dalam upaya mereka untuk mengatasi ancaman ini.

Diadopsi berdasarkan Bab VII Piagam PBB, resolusi ini:

1. Menegaskan kembali bahwa Negara-negara Anggota harus mematuhi kewajiban hak asasi manusia mereka ketika memerangi terorisme dan mencatat bahwa kegagalan untuk melakukannya berkontribusi pada radikalisasi.
2. Mendefinisikan istilah Pejuang Teroris Asing sebagai "orang-orang yang melakukan perjalanan ke suatu Negara selain Negara tempat tinggal atau kebangsaan mereka untuk tujuan melakukan, merencanakan, atau mempersiapkan, atau berpartisipasi dalam, aksi teroris atau menyediakan atau menerima teroris. pelatihan, termasuk yang berhubungan dengan konflik bersenjata."
3. Mengungkapkan keprihatinan khusus tentang FTF yang telah bergabung dengan Negara Islam di Irak dan Syam (ISIL), Front Al-Nusrah, dan kelompok lain yang terkait dengan Al-Qaida.
4. Mengungkapkan keprihatinan atas penggunaan internet untuk menghasut orang lain untuk melakukan tindakan teroris dan menggarisbawahi perlunya mencegah teroris mengeksploitasi teknologi untuk menghasut dukungan untuk tindakan teroris, sementara pada saat yang sama menghormati hak asasi manusia dan kebebasan mendasar.
5. Mencatat pekerjaan badan-badan multilateral lainnya, termasuk INTERPOL dan badan-badan PBB lainnya, dan adopsi baru-baru ini oleh Forum Kontraterorisme Global (GCTF) tentang praktik-praktik baik yang direkomendasikan untuk menanggapi ancaman FTF.
6. Menuntut FTF untuk melucuti dan menghentikan semua tindakan teroris dan partisipasi dalam konflik bersenjata.
7. Menyerukan negara-negara untuk meminta maskapai penerbangan mereka untuk memberikan informasi penumpang terlebih dahulu untuk mendeteksi perjalanan teroris yang terdaftar di PBB.

Kewajiban

8. Mengharuskan negara-negara untuk mencegah dan menekan perekrutan, pengorganisasian, pengangkutan, dan perlengkapan FTF, serta pembiayaan perjalanan dan kegiatan FTF.
9. Mengharuskan negara-negara untuk memiliki undang-undang yang mengizinkan penuntutan:
    - Warga negara mereka dan orang lain yang meninggalkan wilayah mereka yang melakukan perjalanan atau mencoba melakukan perjalanan untuk tujuan terorisme;
    - Penyediaan atau pengumpulan dana yang disengaja oleh warga negara mereka atau di wilayah mereka dengan maksud atau pengetahuan bahwa dana tersebut akan digunakan untuk membiayai perjalanan FTF;
    - Organisasi atau fasilitasi yang disengaja oleh warga negara mereka atau di wilayah mereka untuk perjalanan tersebut.
10. Mengharuskan negara-negara untuk mencegah masuk atau transit individu yang diyakini melakukan perjalanan untuk tujuan terkait terorisme.

Kerjasama internasional

11. Menghimbau negara-negara untuk meningkatkan kerjasama internasional, regional, dan sub-regional untuk mencegah perjalanan FTF, termasuk melalui peningkatan pertukaran informasi.

12. Menyoroti perlunya negara-negara untuk mematuhi kewajiban mereka yang ada terkait kerja sama dalam investigasi dan proses kriminal terkait terorisme sehubungan dengan investigasi dan proses yang melibatkan FTFs.
13. Mendorong INTERPOL untuk mengintensifkan upayanya menanggapi ancaman FTF.
14. Menyerukan negara-negara untuk saling membantu membangun kapasitas untuk mengatasi ancaman FTF dan menyambut baik bantuan bilateral untuk melakukannya.

Melawan Ekstremisme dengan Kekerasan Untuk Mencegah Terorisme

15. Menggarisbawahi bahwa Melawan Ekstremisme Kekerasan (CVE) adalah elemen penting dalam menanggapi ancaman FTF.
16. Menyerukan Negara-negara untuk meningkatkan upaya CVE dan mengambil langkah-langkah untuk mengurangi risiko radikalisasi terorisme di masyarakat mereka, seperti melibatkan komunitas lokal yang relevan, memberdayakan kelompok masyarakat sipil yang peduli, dan mengadopsi pendekatan yang disesuaikan untuk melawan perekrutan FTF.

Keterlibatan PBB

17. Mengarahkan badan kontra-terorisme PBB untuk memusatkan perhatian pada ancaman FTF, memungkinkan masyarakat internasional untuk menilai kepatuhan terhadap resolusi ini dan untuk menargetkan bantuan kepada negara-negara yang membutuhkan bantuan untuk menegakkan ketentuannya.
18. Meminta laporan dari PBB dalam waktu 180 hari untuk menilai secara komprehensif fenomena FTF dan merekomendasikan tindakan untuk meningkatkan respon terhadap ancaman.

16.8 RESOLUSI PENANGGULANGAN TERORISME PBB

Strategi Kontra-Terorisme Global Perserikatan Bangsa-Bangsa diadopsi dengan suara bulat oleh Majelis Umum pada tahun 2006, yang merupakan tonggak sejarah dalam domain inisiatif kontra-terorisme multilateral. Berdasarkan Strategi tersebut, Negara-negara Anggota memutuskan, antara lain:

a) Untuk secara konsisten, tegas dan keras mengutuk terorisme dalam segala bentuk dan manifestasinya, yang dilakukan oleh siapa pun, di mana pun dan untuk tujuan apa pun, karena merupakan salah satu ancaman paling serius bagi perdamaian dan keamanan internasional;
b) Mengambil tindakan segera untuk mencegah dan memerangi terorisme dalam segala bentuk dan manifestasinya;
c) Mengakui bahwa kerja sama internasional dan tindakan apa pun yang [mereka] lakukan untuk mencegah dan memerangi terorisme harus mematuhi kewajiban [mereka] berdasarkan hukum internasional, termasuk Piagam Perserikatan Bangsa-Bangsa dan konvensi serta protokol internasional yang relevan, khususnya hak asasi manusia. hukum, hukum pengungsi dan hukum humaniter internasional;
d) Bekerja dengan Perserikatan Bangsa-Bangsa dengan memperhatikan kerahasiaan, menghormati hak asasi manusia dan sesuai dengan kewajiban lain berdasarkan hukum internasional, untuk mencari cara dan sarana untuk "(a) Mengkoordinasikan upaya di tingkat internasional dan regional untuk melawan terorisme di segala bentuk dan

manifestasinya di Internet; (b) Menggunakan Internet sebagai alat untuk melawan penyebaran terorisme, sambil mengakui bahwa negara mungkin memerlukan bantuan dalam hal ini" [penekanan ditambahkan].

Beberapa resolusi Dewan Keamanan yang diadopsi dalam beberapa tahun terakhir mengharuskan negara-negara untuk bekerja sama sepenuhnya dalam memerangi terorisme, dalam segala bentuknya. Secara khusus, resolusi 1373 (2001) dan 1566 (2004), yang diadopsi berdasarkan Bab VII Piagam Perserikatan Bangsa-Bangsa, mensyaratkan tindakan legislatif dan tindakan lain yang harus diambil oleh semua Negara Anggota untuk memerangi terorisme, termasuk melalui peningkatan kerja sama dengan Pemerintah lain dalam penyelidikan, pendeteksian, penangkapan, ekstradisi dan penuntutan mereka yang terlibat dalam aksi teroris; dan menyerukan kepada Negara-negara untuk menerapkan konvensi dan protokol internasional yang berkaitan dengan terorisme.

Resolusi penting Dewan Keamanan lainnya yang berkaitan dengan aktivitas teroris yang dapat dilakukan melalui Internet adalah resolusi 1624 (2005), yang membahas hasutan dan pemuliaan tindakan teroris. Dalam paragraf pembukaan keempat, dewan mengutuk "dalam istilah yang paling kuat hasutan tindakan teroris "dan menolak" upaya pembenaran atau pemuliaan (permintaan maaf) dari tindakan teroris yang dapat memicu tindakan teroris lebih lanjut". Dalam paragraf 1, Ia menyerukan kepada semua negara untuk mengambil tindakan-tindakan yang mungkin diperlukan dan sesuai, dan sesuai dengan kewajiban mereka menurut hukum internasional, untuk melarang oleh hukum dan mencegah hasutan untuk melakukan tindakan atau tindakan teroris.

Laporan dan resolusi PBB baru-baru ini secara khusus mengakui pentingnya melawan penggunaan Internet oleh teroris sebagai bagian penting dari strategi kontra-terorisme yang komprehensif. Dalam laporannya tahun 2006 kepada Majelis Umum berjudul "bersatu melawan terorisme: rekomendasi untuk strategi kontra-terorisme global", sekretaris jenderal secara eksplisit menyatakan: "kemampuan untuk menghasilkan dan menggerakkan keuangan, untuk memperoleh senjata, merekrut dan melatih kader, dan untuk berkomunikasi, terutama melalui penggunaan Internet, semuanya penting bagi teroris. "Sekretaris Jenderal melanjutkan dengan menegaskan bahwa Internet adalah kendaraan yang berkembang pesat untuk perekrutan teroris dan penyebaran informasi dan propaganda, yang harus dilawan melalui tindakan terkoordinasi oleh Negara-negara Anggota, sambil menghormati hak asasi manusia dan kewajiban lain di bawah hukum internasional.

Dalam resolusinya 1963 (2010), Dewan Keamanan menyatakan "keprihatinan pada peningkatan penggunaan, dalam masyarakat global, oleh teroris teknologi informasi dan komunikasi baru, khususnya Internet, untuk tujuan perekrutan dan penghasutan serta untuk pembiayaan, perencanaan dan persiapan kegiatan mereka." Dewan juga mengakui pentingnya kerjasama di antara Negara-negara Anggota untuk mencegah teroris mengeksploitasi teknologi, komunikasi dan sumber daya.

16.9 KERANGKA KEBIJAKAN DAN LEGISLATIF

Untuk memberikan tanggapan peradilan pidana yang efektif terhadap ancaman yang dihadirkan oleh teroris yang menggunakan Internet, Negara memerlukan kebijakan nasional

dan kerangka kerja legislatif yang jelas. Secara garis besar, kebijakan dan undang-undang tersebut akan berfokus pada:

a) Kriminalisasi tindakan melanggar hukum yang dilakukan oleh teroris melalui Internet atau layanan terkait;
b) Pemberian wewenang investigasi bagi lembaga penegak hukum yang terlibat dalam investigasi terkait terorisme;
c) Regulasi layanan terkait Internet (misalnya ISP) dan kontrol konten;
d) Fasilitasi kerjasama internasional;
e) Pengembangan prosedur peradilan atau pembuktian khusus;
f) Pemeliharaan standar hak asasi manusia internasional.

PBB dalam publikasi 2011, Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects, the Working Group on Countering the Use of Internet for Terrorist Purposes of the Counter-Terrorism Implementation Task Force mengidentifikasi tiga pendekatan strategis yang luas yang dapat digunakan oleh Negara melawan aktivitas teroris melalui Internet; melibatkan penggunaan:

a) Undang-undang kejahatan dunia maya umum;
b) Perundang-undangan kontra-terorisme umum (non-internet-spesifik);
c) Undang-undang kontra-terorisme khusus Internet

Sumber daya lain yang berguna bagi pembuat kebijakan dan pembuat undang-undang, yang dirujuk dalam Melawan Penggunaan Internet untuk Tujuan Teroris adalah Perangkat untuk Perundang-undangan Kejahatan Dunia Maya, yang dikembangkan di bawah naungan ITU. Selain model ketentuan pidana lainnya, Toolkit ini berisi beberapa pelanggaran khusus terkait teroris, termasuk bagian 3 (f), yang berhubungan dengan akses tidak sah ke, atau memperoleh program komputer untuk, tujuan mengembangkan, merumuskan, merencanakan, memfasilitasi, membantu dalam melakukan, bersekongkol untuk melakukan atau melakukan tindakan terorisme.

16.10 STUDI KASUS INGGRIS

R v. Tsouli dan lainnya: Kasus terkenal dari Inggris ini melibatkan tiga terdakwa—Younes Tsouli, Waseem Mughal dan Tariq al-Daour—yang awalnya didakwa atas 15 dakwaan. Sebelum diadili, Tsouli dan Mughal mengaku bersalah atas tuduhan konspirasi untuk menipu. Selama persidangan, setelah mendengar bukti penuntutan, ketiganya mengaku bersalah atas tuduhan menghasut terorisme di luar negeri, dan Al-Daour mengaku bersalah atas tuduhan konspirasi untuk menipu.

Antara Juni 2005 dan penangkapan mereka pada Oktober 2005, para terdakwa terlibat dalam pembelian, pembangunan, dan pemeliharaan sejumlah besar situs web dan forum obrolan Internet yang memuat materi yang memicu tindakan pembunuhan teroris, terutama di Irak. Biaya pembelian dan pemeliharaan situs web dipenuhi dari hasil penipuan kartu kredit. Materi di situs web termasuk pernyataan bahwa adalah kewajiban umat Islam untuk melakukan jihad bersenjata melawan orang Yahudi, tentara salib, murtad dan pendukung mereka di semua negara Muslim dan bahwa adalah tugas setiap Muslim untuk memerangi dan membunuh mereka di mana pun mereka berada, warga sipil. atau militer. Di forum-forum obrolan Internet, orang-orang yang bersedia bergabung dengan pemberontakan diberikan

rute untuk melakukan perjalanan ke Irak dan manual tentang resep senjata dan bahan peledak.

Materi ideologis ekstrem yang menunjukkan kepatuhan pada pembenaran yang dianut untuk tindakan pembunuhan yang dihasut oleh situs web dan forum obrolan ditemukan dari rumah masing-masing terdakwa. Al-Daour mengatur perolehan kartu kredit curian, baik untuk keperluannya sendiri maupun untuk menyediakan dana bagi Mughal untuk menyiapkan dan menjalankan situs web. Al-Daour juga terlibat dalam penipuan kartu kredit lebih lanjut; yang hasilnya tidak digunakan untuk mendukung situs web. Kerugian perusahaan kartu kredit dari aspek aktivitas penipuan terdakwa adalah 1,8 juta Poundsterling.

Di antara buktinya adalah daftar yang dibuat oleh Tsouli dengan tulisan tangannya dan ditemukan di mejanya di mana ia telah menulis rincian sejumlah situs web dan kartu kredit curian. Ini mengungkapkan 32 situs web terpisah yang disediakan oleh sejumlah perusahaan hosting web berbeda yang telah atau coba didirikan oleh Tsouli, sebagian besar pada minggu terakhir Juni 2005 tetapi berlanjut hingga Juli dan Agustus. Pembuatan dan administrasi situs web ini didanai oleh penipuan penggunaan rincian kartu kredit yang telah dicuri dari pemegang rekening, baik dengan pencurian langsung catatan komputer, dengan hacking atau oleh beberapa pengalihan penipuan dalam lembaga keuangan. Rincian kartu kredit ini telah diteruskan ke Tsouli oleh dua terdakwa lainnya.

Situs web yang dibuat oleh Tsouli digunakan sebagai sarana untuk mengunggah materi jihad, yang memicu tindakan kekerasan di luar Inggris di Irak. Akses ke situs dibatasi untuk mereka yang telah diberikan nama pengguna dan kata sandi. Hal ini dilakukan, hakim pengadilan menemukan, untuk membuat lebih sulit bagi perusahaan web-hosting dan lembaga penegak hukum untuk mengetahui apa yang sedang diposting di situs. Pada tanggal 5 Juli 2007, Tsouli dijatuhi hukuman 10 tahun penjara dan 3½ tahun (bersamaan) atas dua dakwaan. Mughal hingga 7½ tahun penjara dan 3½ tahun (bersamaan) pada dua dakwaan dan al-Daour, hingga 6½ tahun penjara dan 3½ tahun (bersamaan).

16.11 RINGKASAN

Konsep hak asasi manusia dalam perspektif teroris dunia maya sedikit berbeda secara global dan beberapa waktu mereka mengklaim diri sebagai pejuang kebebasan dan berjuang untuk tujuan agama. Dalam unit ini konsep penting cyber terrorism dan HAM berupa konvensi internasional tentang terorisme, cyber terrorism dan hak privasi, HAM dan UDHR, HAM, PBB dan dunia cyber, kebijakan luar negeri dan kerangka legislatif serta studi kasus. Inggris dibahas panjang lebar untuk memahami masalah.

16.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Authorpress)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)

- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang tepat dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

16.13 PERIKSA KEMAJUANMU

A. Manakah dari pernyataan berikut ini yang benar atau salah:
   a Isu terorisme dan hak asasi manusia telah lama menjadi perhatian PBB.
   b Hak atas privasi sebagai konsep yang independen dan khas berasal dari bidang hukum gugatan.
   c Perlindungan HAM di ruang siber sangat dibutuhkan di tingkat nasional dan nasional.
   d Strategi Kontra Terorisme Global PBB diadopsi dengan suara bulat oleh Majelis Umum pada tahun 2006.
   e Resolusi 2178 mengharuskan negara-negara untuk mengambil langkah-langkah tertentu untuk mengatasi FTF (Foreign Terrorist Fighters).

B. Isi Bagian yang Kosong:
   I. Memperluas penyelenggara …….. bandar udara penerbangan sipil internasional.
   II. …… Konvensi Internasional untuk Pemberantasan Bom Teroris terkait dengan Konvensi Pengeboman Teroris.
   III. ……. Konvensi Internasional untuk Pemberantasan Tindakan Nuklir terkait dengan Terorisme (Konvensi Terorisme Nuklir).
   IV. …….. dari Deklarasi Universal Hak Asasi Manusia menetapkan hak atas “keamanan pribadi”.

V. Resolusi Dewan Keamanan PBB No. 2178 terkait dengan ……..

16.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Konvensi Montreal
2. 1997
3. 2005
4. Pasal 3
5. Pejuang Teroris Asing

16.15 PERTANYAAN TERMINAL

1. Berapa banyak Konvensi Internasional tentang Terorisme?
2. Definisikan terorisme dan hak atas privasi.
3. Apa resolusi PBB No. 2178?
4. Apa itu Resolusi Penanggulangan Terorisme PBB?
5. Tulis studi kasus di Inggris?

BAB 17
PERAN ORGANISASI INTERNASIONAL DALAM KEJAHATAN CYBER

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami isu-isu dan pokok bahasan di bawah lingkup Organisasi Internasional dengan mengacu pada Kejahatan Cyber
- Memahami peran dan pentingnya berbagai Organisasi internasional dalam Memerangi Kejahatan Dunia Maya
- Memahami masalah teknis dan hukum yang terkait dengan Kejahatan Cyber

17.1 PENGANTAR

Pada tahun 2011, setidaknya 2,3 miliar orang, setara dengan lebih dari sepertiga dari total populasi dunia, memiliki akses ke internet. Lebih dari 60 persen pengguna internet berada di negara berkembang, dengan 45 persen dari semua pengguna internet berusia di bawah 25 tahun. Pada tahun 2017, diperkirakan langganan mobile broadband akan mendekati 70 persen dari total populasi dunia. Pada tahun 2020, jumlah perangkat jaringan (internet of things) akan melebihi jumlah orang sebanyak enam banding satu, mengubah konsepsi internet saat ini. Di dunia masa depan yang sangat terhubung, akan sulit membayangkan 'kejahatan komputer', dan mungkin kejahatan apa pun, yang tidak melibatkan bukti elektronik yang terkait dengan konektivitas protokol internet (IP). 'Definisi' kejahatan dunia maya sebagian besar bergantung pada tujuan penggunaan istilah tersebut. Sejumlah terbatas tindakan terhadap kerahasiaan, integritas dan ketersediaan data atau sistem komputer merupakan inti dari kejahatan dunia maya.

Di luar ini, bagaimanapun, tindakan terkait komputer untuk keuntungan atau kerugian pribadi atau finansial, termasuk bentuk kejahatan terkait identitas, dan tindakan terkait konten komputer (semuanya termasuk dalam arti yang lebih luas dari istilah 'kejahatan dunia maya') tidak diri mereka sendiri dengan mudah ke upaya untuk sampai pada definisi hukum dari istilah agregat. Definisi tertentu diperlukan untuk inti dari tindakan kejahatan dunia maya. Namun, 'definisi' kejahatan dunia maya tidak relevan untuk tujuan lain, seperti mendefinisikan ruang lingkup investigasi khusus dan kekuatan kerjasama internasional, yang lebih fokus pada bukti elektronik untuk kejahatan apa pun, daripada 'kejahatan dunia maya' yang luas dan artifisial.

Lebih dari 90 persen negara yang menanggapi melaporkan bahwa tindakan kejahatan dunia maya paling sering menjadi perhatian otoritas penegak hukum melalui laporan oleh korban individu atau perusahaan. Negara-negara yang menanggapi memperkirakan bahwa proporsi korban kejahatan dunia maya yang dilaporkan ke polisi berkisar antara 1 persen. Satu survei sektor swasta global menunjukkan bahwa 80 persen individu korban kejahatan dunia maya inti tidak melaporkan kejahatan tersebut kepada polisi. Underreporting berasal dari kurangnya kesadaran viktimisasi dan mekanisme pelaporan, rasa malu dan malu korban, dan risiko reputasi yang dirasakan bagi perusahaan. Pihak berwenang di seluruh wilayah dunia menyoroti inisiatif untuk meningkatkan pelaporan, termasuk sistem pelaporan online dan

hotline, kampanye kesadaran publik, hubungan sektor swasta, dan peningkatan jangkauan polisi dan berbagi informasi.

Namun, respons yang didorong oleh insiden terhadap kejahatan dunia maya harus disertai dengan investigasi taktis jangka menengah dan panjang yang berfokus pada pasar kejahatan dan arsitek skema kriminal. Otoritas penegak hukum di negara maju terlibat dalam bidang ini, termasuk melalui unit penyamaran yang menargetkan pelanggar di situs jejaring sosial, ruang obrolan, dan pesan instan serta layanan P2P. Tantangan dalam penyidikan kejahatan dunia maya muncul dari inovasi kriminal oleh pelaku, kesulitan dalam mengakses bukti elektronik, dan dari sumber daya internal, kapasitas dan keterbatasan logistik. Tersangka sering menggunakan teknologi anonimisasi dan penyamaran, dan teknik baru dengan cepat menjangkau khalayak kriminal yang luas melalui pasar kejahatan online.

17.2 INTERPOL DAN KEJAHATAN CYBER

Kejahatan dunia maya adalah area kejahatan yang berkembang pesat. Semakin banyak penjahat yang mengeksploitasi kecepatan, kenyamanan dan anonimitas Internet untuk melakukan beragam kegiatan kriminal yang tidak mengenal batas, baik fisik maupun virtual.
Kejahatan-kejahatan ini dapat dibagi menjadi tiga bidang besar:

- Serangan terhadap perangkat keras dan perangkat lunak komputer, misalnya botnet, malware, dan intrusi jaringan;
- Kejahatan keuangan, seperti penipuan online, penetrasi layanan keuangan online, dan phishing;

Pelecehan, terutama terhadap kaum muda, dalam bentuk dandanan atau “eksploitasi”. Tren baru dalam kejahatan dunia maya muncul setiap saat, dengan biaya ekonomi global mencapai miliaran dolar.

Di masa lalu, kejahatan dunia maya dilakukan terutama oleh individu atau kelompok kecil. Hari ini, kita melihat organisasi kriminal bekerja dengan profesional teknologi yang berpikiran kriminal untuk melakukan kejahatan dunia maya, seringkali untuk mendanai kegiatan ilegal lainnya. Sangat kompleks, jaringan kejahatan dunia maya ini menyatukan individu-individu dari seluruh dunia secara real time untuk melakukan kejahatan dalam skala yang belum pernah terjadi sebelumnya.

Organisasi kriminal semakin beralih ke Internet untuk memfasilitasi aktivitas mereka dan memaksimalkan keuntungan mereka dalam waktu singkat. Kejahatan itu sendiri tidak selalu baru – seperti pencurian, penipuan, perjudian ilegal, penjualan obat-obatan palsu – tetapi mereka berkembang sejalan dengan peluang yang disajikan secara online dan oleh karena itu menjadi lebih luas dan merusak.

Peran INTERPOL: INTERPOL berkomitmen untuk menjadi badan koordinasi global dalam pendeteksian dan pencegahan kejahatan digital melalui INTERPOL Global Complex for Innovation (IGCI), yang saat ini sedang dibangun di Singapura. Komponen kunci dari fasilitas penelitian dan pengembangan mutakhir yang baru ini adalah INTERPOL Digital Crime Centre. Pusat baru ini menyediakan penelitian proaktif ke area baru dan teknik pelatihan terbaru, dan mengoordinasikan operasi di lapangan.
Inisiatif utama kami dalam kejahatan dunia maya berfokus pada:

- Peningkatan kapasitas Harmonisasi

- Dukungan operasional dan forensik.

Sementara penegakan hukum yang efektif merupakan komponen penting untuk memerangi ancaman dunia maya, kami juga menyadari pentingnya melibatkan semua pemangku kepentingan – dari sektor swasta, akademisi, dan lembaga publik – yang bekerja menuju tujuan bersama dari ruang maya yang lebih aman.

Penting untuk menyelaraskan upaya lintas sektor yang berbeda untuk berbagi keahlian sambil menghindari duplikasi kegiatan yang sudah berjalan. Dengan cara ini, polisi dapat secara efisien memfokuskan sumber daya mereka untuk memerangi kejahatan dunia maya, karena kami bekerja dengan pemangku kepentingan lain untuk mengembangkan respons yang holistik dan terkoordinasi.

Dengan mendorong pembentukan unit investigasi kejahatan dunia maya khusus, dan memperbarui kerangka hukum, INTERPOL akan membangun peran fasilitasi proaktif dalam memerangi kejahatan dunia maya.

Layanan utama dari harmonisasi meliputi:

- Tinjauan dunia maya nasional – audit komprehensif terhadap undang-undang nasional, infrastruktur kepolisian, dan kapasitas teknis, dengan rekomendasi yang menyertainya; Pengembangan strategi keamanan siber – bekerja dengan badan pengatur untuk mengembangkan strategi global serta memberikan saran kepada masing-masing negara tentang pendekatan nasional mereka;
- Advokasi internasional tentang undang-undang dan tata kelola dunia maya – mewakili perspektif penegakan hukum dalam pengembangan undang-undang baru dan yang diperbarui; Penelitian dan inovasi – menggabungkan penelitian kepolisian dengan kegiatan serupa di sektor lain.

Di INTERPOL, kami bekerja untuk memastikan bahwa polisi mengikuti perkembangan teknologi dan memiliki keahlian dan keterampilan yang diperlukan untuk menangani kejahatan digital yang berkembang di tingkat nasional dan internasional. Kami menyediakan berbagai kursus pelatihan, yang ditargetkan untuk kebutuhan peserta, mencakup topik-topik seperti tren yang muncul dalam kejahatan dunia maya, teknik investigasi, forensik digital, dan banyak lagi. Pelatihan berbentuk modul e-learning, sesi dan lokakarya berbasis kelas dan dapat mengarah pada sertifikasi profesional. Kursus 'train-the-trainer' sangat berharga karena memungkinkan peserta untuk menyampaikan keterampilan dan pengetahuan baru mereka kepada rekan-rekan mereka.

Semakin banyak, portofolio pelatihan pelatihan kejahatan dunia maya INTERPOL dikembangkan dan disampaikan dengan masukan dari akademisi, tim tanggap darurat komputer (CERT), kepolisian nasional dan sektor swasta. Kami mendukung negara-negara anggota selama investigasi dunia maya dan membantu mengoordinasikan operasi bersama.

Pusat Fusi Cyber

Ini memberikan bantuan penting kepada negara-negara anggota INTERPO selama semua tahap penyelidikan. Berfungsi Dengan cara yang mirip dengan Pusat Komando dan Koordinasi INTERPOL, Cyber Fusion Center menyediakan pemantauan dan analisis real-time dari aktivitas internet berbahaya, memberikan negara-negara anggota intelijen dan keahlian yang dibutuhkan untuk lebih efektif menyelidiki kejahatan digital.

Laboratorium Forensik Digital

Laboratorium ini bekerja untuk membangun kapasitas forensik digital nasional melalui pelatihan, sekaligus memberikan dukungan forensik praktis kepada negara-negara anggota selama penyelidikan.

Koordinasi wilayah

Kelompok Kerja telah dibentuk untuk memfasilitasi pengembangan strategi regional, teknologi dan informasi tentang tren dan metode kejahatan terbaru.

Ada partai kerja regional untuk:

- Afrika
- Amerika
- Eropa dan Asia
- Timur Tengah dan Afrika Utara.

Kegiatan utama dari pihak-pihak yang bekerja didasarkan pada operasi, pelatihan dan mencari solusi untuk ancaman yang muncul.

17.3 BIRO INVESTIGASI FEDERAL (FBI) DAN KEJAHATAN CYBER-I

Intrusi Komputer

Setiap hari, penjahat menyerang rumah dan kantor yang tak terhitung jumlahnya di seluruh negeri—bukan dengan mendobrak jendela dan pintu, tetapi dengan membobol laptop, komputer pribadi, dan perangkat nirkabel melalui peretasan dan potongan kode berbahaya. Dampak kolektifnya luar biasa. Miliaran dolar hilang setiap tahun untuk memperbaiki sistem yang terkena serangan semacam itu. Beberapa menghancurkan sistem vital, mengganggu dan terkadang melumpuhkan pekerjaan rumah sakit, bank, dan layanan 9-1-1 di seluruh negeri.

Siapa di balik serangan seperti itu? Ini menjalankan keseluruhan—dari geek komputer yang mencari hak untuk menyombongkan diri… hingga bisnis yang mencoba meraih keunggulan di pasar dengan meretas situs web pesaing, dari jaringan penjahat yang ingin mencuri informasi pribadi Anda dan menjualnya di pasar gelap … hingga mata-mata dan teroris ingin merampok informasi penting negara kita atau meluncurkan serangan dunia maya.

Saat ini, kasus penyusupan komputer ini—kontraterorisme, kontra intelijen, dan kriminal—merupakan prioritas utama program siber kami karena potensi hubungannya dengan keamanan nasional. Memerangi ancaman. Dalam beberapa tahun terakhir, kami telah membangun serangkaian kapabilitas dan kemitraan teknologi dan investigasi yang benar-benar baru—sehingga kami sama nyamannya mengejar penjahat di dunia maya seperti halnya kami berada di gang-gang kecil dan lintas benua. Itu termasuk:

- Divisi Siber di Markas Besar FBI “untuk menangani kejahatan siber secara terkoordinasi dan kohesif”.
- Pasukan siber yang terlatih secara khusus di markas besar FBI dan di masing-masing dari 56 kantor lapangan kami, dengan staf “agen dan analis yang melindungi dari investigasi intrusi komputer, pencurian kekayaan intelektual dan informasi pribadi, pornografi dan eksploitasi anak, dan penipuan online”:
- Tim Aksi Siber Baru yang “bepergian ke seluruh dunia dalam waktu singkat untuk membantu dalam kasus penyusupan komputer dan bahwa” intelijen vital yang

membantu kita mengidentifikasi kejahatan siber yang paling berbahaya bagi keamanan nasional dan ekonomi kita:"

- 93 Satuan Tugas Kejahatan Komputer kami di seluruh negeri yang "menggabungkan teknologi canggih dan sumber daya dari mitra federal, negara bagian, dan lokal kami".
- Kemitraan yang berkembang dengan lembaga federal lainnya, termasuk Departemen Pertahanan, Departemen Keamanan Dalam Negeri, dan lainnya—yang memiliki keprihatinan dan tekad yang sama dalam memerangi kejahatan dunia maya.

17.4 BIRO INVESTIGASI FEDERAL (FBI) DAN KEJAHATAN CYBER-II

Tips Belanja Liburan: FBI mengingatkan pembeli liburan untuk waspada terhadap penjahat cyber yang keluar untuk mencuri uang dan informasi pribadi. Penipu menggunakan banyak teknik untuk menipu konsumen, mulai dari email phishing yang menawarkan penawaran yang terlalu bagus untuk menjadi kenyataan pada barang dagangan bermerek hingga menawarkan uang tunai cepat kepada korban yang akan mengirimkan kembali paket ke tujuan tambahan. Penipuan yang dilaporkan sebelumnya masih dilakukan hari ini.

Meskipun memantau laporan kredit setiap tahun dan meninjau laporan rekening setiap bulan selalu merupakan ide yang baik, konsumen harus tetap waspada terhadap informasi kredit pribadi mereka saat ini sepanjang tahun. Meneliti tagihan kartu kredit untuk setiap aktivitas penipuan dapat membantu meminimalkan kerugian korban. Tagihan yang tidak dapat dikenali yang tercantum pada laporan kartu kredit sering kali pertama kali konsumen menyadari bahwa informasi pengenal pribadi mereka telah dicuri.

Transaksi bank dan korespondensi dari lembaga keuangan juga harus ditinjau dengan cermat. Rekening bank sering kali menjadi sasaran para penjahat untuk memulai pengambilalihan rekening atau melakukan pencurian identitas dengan membuat rekening baru atas nama korban. nasabah tidak boleh mengklik link yang disematkan dalam email dari bank mereka, melainkan membuka halaman web baru dan memasukkan URL (alamat web) secara manual, karena penipuan phishing sering dimulai dengan email palsu yang menampilkan nama dan logo bank.

Saat berbelanja online, pastikan untuk menggunakan situs yang memiliki reputasi baik. Seringkali konsumen diperlihatkan penawaran khusus di web, atau bahkan dalam penawaran email, yang kelihatannya terlalu bagus untuk menjadi kenyataan. Situs-situs ini digunakan untuk menangkap informasi pengenal pribadi, termasuk nomor kartu kredit, alamat, dan nomor telepon untuk melakukan transaksi penipuan. Sebaiknya berbelanja di situs yang Anda kenal dan yang memiliki reputasi mapan sebagai pengecer online tepercaya, menurut MRC, organisasi nirlaba yang mendukung dan mempromosikan keunggulan operasional untuk profesional penipuan, pembayaran, dan risiko dalam e-Commerce.

Jika Anda mencari item atau nama perusahaan melalui situs mesin pencari, teliti hasil yang terdaftar sebelum pergi ke situs web. Jangan secara otomatis mengklik hasil pertama, meskipun terlihat identik atau mirip dengan hasil yang diinginkan. Banyak penipu berusaha keras agar situs web mereka sendiri muncul di depan perusahaan yang sah di mesin pencari populer. Situs web mereka mungkin merupakan versi cermin dari situs web populer, tetapi dengan URL yang sedikit berbeda.

Pembelian yang dilakukan di situs-situs ini dapat mengakibatkan satu atau beberapa konsekuensi berikut: tidak pernah menerima item, rincian kartu kredit Anda dicuri, atau mengunduh malware/virus komputer ke komputer Anda. Sebelum mengeklik hasil di mesin telusur, periksa URL situs web tujuan. Cari kesalahan ejaan atau karakter tambahan seperti titik atau koma karena ini merupakan indikasi penipuan. Saat dibawa ke halaman pembayaran situs web, verifikasi lagi URL dan pastikan itu aman dengan memulai dengan "HTTPS" bukan hanya "HTTP".

Berikut adalah beberapa tips tambahan yang dapat Anda gunakan untuk menghindari menjadi korban penipuan cyber:

- Jangan menanggapi email yang tidak diminta (spam).
- Jangan mengklik link yang terdapat dalam email yang tidak diinginkan.
- Berhati-hatilah terhadap e-mail yang mengklaim berisi gambar dalam file terlampir; file mungkin berisi virus. Hanya buka lampiran dari pengirim yang dikenal. Pindai lampiran untuk virus jika memungkinkan.
- Hindari mengisi formulir yang terdapat dalam pesan email yang meminta informasi pribadi.
- Selalu bandingkan tautan dalam email dengan tautan yang sebenarnya Anda tuju dan tentukan apakah tautan tersebut cocok dan akan mengarahkan Anda ke situs yang sah.
- Masuk langsung ke situs web resmi untuk bisnis yang diidentifikasi dalam email alih-alih "menautkan" ke sana dari email yang tidak diminta. Jika email tersebut tampaknya berasal dari bank, penerbit kartu kredit, atau perusahaan lain yang sering Anda tangani, pernyataan atau korespondensi resmi dari bisnis tersebut akan memberikan informasi kontak yang tepat.
- Hubungi bisnis sebenarnya yang seharusnya mengirim email untuk memverifikasi bahwa email tersebut asli.
- Jika Anda diminta untuk bertindak cepat atau ada keadaan darurat yang membutuhkan perhatian Anda, itu mungkin scam. Penipu menciptakan rasa urgensi untuk membuat Anda bertindak cepat.
- Ingat jika kelihatannya terlalu bagus untuk menjadi kenyataan, mungkin memang begitu.

17.5 BIRO INVESTIGASI FEDERAL (FBI) DAN KEJAHATAN CYBER- III

Penipuan Internet: Di bawah ini adalah tips untuk melindungi diri Anda dan keluarga Anda dari berbagai bentuk penipuan Internet. Untuk informasi tentang keluhan dan penipuan yang paling umum, lihat laporan tahunan Pusat Pengaduan Kejahatan Internet, atau IC3, kemitraan FBI dan Pusat Kejahatan Kerah Putih Nasional. Lihat juga informasi tentang Skema Kejahatan Internet dan Tips Pencegahan Kejahatan Internet. Gunakan formulir kiat online kami atau situs web IC3 untuk melaporkan kemungkinan kasus penipuan dunia maya.

Tips Menghindari Penipuan Lelang Internet:

- Pahami sebanyak mungkin tentang cara kerja lelang, apa kewajiban Anda sebagai pembeli, dan apa kewajiban penjual sebelum Anda menawar.
- Cari tahu tindakan apa yang diambil situs web/perusahaan jika terjadi masalah dan pertimbangkan untuk mengasuransikan transaksi dan pengiriman.

- Pelajari sebanyak mungkin tentang penjual, terutama jika satu-satunya informasi yang Anda miliki adalah alamat email. Jika itu adalah bisnis, periksa Better Business Bureau di mana penjual/bisnis berada.
- Periksa umpan balik pada penjual.
- Tentukan metode pembayaran apa yang diminta penjual dari pembeli dan ke mana dia meminta untuk mengirim pembayaran.
- Jika memungkinkan, beli barang secara online menggunakan kartu kredit Anda, karena Anda sering kali dapat membantah tagihan jika terjadi kesalahan.
- Berhati-hatilah saat berurusan dengan penjual di luar Amerika Serikat. Jika terjadi masalah dengan transaksi lelang, akan jauh lebih sulit untuk memperbaikinya.
- Tanyakan kepada penjual tentang kapan pengiriman dapat diharapkan dan apakah barang tersebut dilindungi oleh garansi atau dapat ditukar jika ada masalah.
- Pastikan tidak ada biaya tak terduga, termasuk apakah pengiriman dan penanganan sudah termasuk dalam harga lelang.
- Seharusnya tidak ada alasan untuk memberikan nomor jaminan sosial atau nomor SIM Anda kepada penjual.
- Tips untuk Menghindari Barang Tidak Terkirim:
- Pastikan Anda membeli barang dagangan dari sumber terpercaya.
- Kerjakan pekerjaan rumah Anda pada individu atau perusahaan untuk memastikan bahwa mereka sah.
- Dapatkan alamat fisik daripada sekadar kotak pos dan nomor telepon, dan hubungi penjual untuk melihat apakah nomor telepon itu benar dan berfungsi.
- Kirim e-mail ke penjual untuk memastikan alamat e-mail aktif, dan waspada terhadap mereka yang menggunakan layanan e-mail gratis di mana mobil kredit diperlukan untuk membuka rekening.
- Pertimbangkan atau beli dari penjual yang tidak akan memberi Anda jenis informasi ini
- Periksa dengan Better Businnes Bureau dari area penjual.
- Periksa situs web lain tentang orang/perusahaan ini.
- Jangan menilai seseorang atau perusahaan dari situs web mereka. Situs web yang mencolok dapat diatur dengan cepat.
- Berhati-hatilah saat menanggapi penawaran investasi khusus, terutama melalui email yang tidak diminta.
- Berhati-hatilah saat berhadapan dengan individu/perusahaan dari luar negara Anda sendiri.
- Tanyakan tentang pengembalian dan jaminan.
- Jika memungkinkan, beli barang secara online menggunakan kartu kredit Anda, karena Anda sering kali dapat membantah tagihan jika terjadi kesalahan.
- Pastikan transaksi aman saat Anda mengirimkan nomor kartu kredit Anda secara elektronik.
- Pertimbangkan untuk menggunakan escrow atau layanan pembayaran alternatif.
- Tips Menghindari Penipuan Kartu Kredit:
- Jangan memberikan nomor kartu kredit Anda secara online kecuali situs tersebut aman dan memiliki reputasi baik. Terkadang ikon kecil gembok muncul untuk melambangkan

tingkat keamanan yang lebih tinggi untuk mengirimkan data. Ikon ini bukan jaminan situs yang aman, tetapi memberikan jaminan.

- Jangan mempercayai situs hanya karena mengklaim aman.
- Sebelum menggunakan situs, periksa perangkat lunak keamanan/enkripsi yang digunakannya.
- Pastikan Anda membeli barang dagangan dari sumber terpercaya.
- Kerjakan pekerjaan rumah Anda pada individu atau perusahaan untuk memastikan bahwa mereka sah.
- Dapatkan alamat fisik daripada sekadar kotak pos dan nomor telepon, dan hubungi penjual untuk melihat apakah nomor telepon itu benar dan berfungsi.
- Kirim email ke penjual untuk memastikan alamat email aktif, dan waspadai mereka yang menggunakan layanan email gratis di mana kartu kredit tidak diperlukan untuk membuka akun.
- Pertimbangkan untuk tidak membeli dari penjual yang tidak akan memberi Anda jenis informasi ini.
- Periksa dengan Bisnis yang lebih baik dari area penjual.
- Periksa situs web lain tentang orang/perusahaan ini.
- Jangan menilai pearson atau perusahaan dari situs web mereka. Situs web yang mencolok dapat diatur dengan cepat.
- Berhati-hatilah saat menanggapi penawaran investasi khusus, terutama melalui email yang tidak diminta.
- Berhati-hatilah saat berhadapan dengan individu/perusahaan dari luar negara Anda sendiri.
- Jika memungkinkan, beli barang secara online menggunakan kartu kredit Anda, karena Anda sering kali dapat membantah tagihan jika terjadi kesalahan.
- Pastikan transaksi aman saat Anda mengirimkan nomor kartu kredit Anda secara elektronik.
- Simpan daftar semua kartu kredit dan informasi rekening Anda bersama dengan informasi kontak penerbit kartu. Jika ada sesuatu yang mencurigakan atau Anda kehilangan kartu kredit, segera hubungi penerbit kartu.
- Tips Menghindari Penipuan Investasi:
- Jangan menilai seseorang atau perusahaan dari situs web mereka. Situs web yang mencolok dapat diatur dengan cepat.
- Jangan berinvestasi pada apa pun yang tidak sepenuhnya Anda yakini. Kerjakan pekerjaan rumah Anda pada investasi dan perusahaan untuk memastikan bahwa mereka sah.
- Periksa situs web lain tentang orang/perusahaan ini.
- Berhati-hatilah saat menanggapi penawaran investasi khusus, terutama melalui email yang tidak diminta.
- Berhati-hatilah saat berhadapan dengan individu/perusahaan dari luar negara Anda sendiri.
- Tanyakan tentang semua syarat dan ketentuan.
- Tips Menghindari Penipuan Bisnis:

- Beli barang dagangan dari dealer atau perusahaan terkemuka.
- Dapatkan alamat fisik daripada sekadar kotak pos dan nomor telepon, dan hubungi penjual untuk melihat apakah nomor telepon itu benar dan berfungsi.
- Kirim email ke penjual untuk memastikan alamat email aktif, dan waspadai mereka yang menggunakan layanan email gratis di mana kartu kredit tidak diperlukan untuk membuka akun.
- Pertimbangkan untuk tidak membeli dari penjual yang tidak akan memberi Anda jenis informasi ini.
- Membeli barang dagangan langsung dari individu/perusahaan yang memegang merek dagang, hak cipta, atau paten.
- Kiat untuk Menghindari Penipuan Surat Nigeria atau "419":
- Bersikaplah skeptis terhadap individu yang mewakili diri mereka sebagai pejabat pemerintah Nigeria atau asing yang meminta bantuan Anda untuk menempatkan sejumlah besar uang di rekening bank luar negeri.
- Jangan percaya janji uang dalam jumlah besar untuk kerjasama Anda.
- Jaga informasi akun Anda dengan hati-hati.

17.6 MEMERANGI INDUSTRIALISASI KEJAHATAN CYBER

Ketika kita berbicara tentang ekonomi bawah tanah digital, yang kami maksud adalah kumpulan jaringan global mandiri yang beroperasi sebagian besar di forum Internet tertutup dan memfasilitasi serangkaian kejahatan dunia maya termasuk serangan perbankan, penipuan kartu pembayaran, pencurian identitas, dan gangguan online lainnya. Data pribadi dan keuangan yang dicuri dijual di forum ini.

Kecanggihan model bisnis kriminal ini sedemikian rupa sehingga anggota jaringan ini dapat fokus pada tugas-tugas tertentu termasuk memproduksi kode berbahaya atau mekanisme pengiriman untuk serangan. Bahkan ada spesialis yang berdedikasi pada pembuatan nomor otentikasi kartu pembayaran dan perekrutan bagal uang, individu yang mengubah hasil kejahatan dunia maya menjadi uang tunai—kadang-kadang tanpa mengetahui bahwa mereka terlibat dalam aktivitas kriminal.

Bisnis cybercriminal terus berinovasi. Selain memanfaatkan media sosial secara ekstensif untuk mendistribusikan penipuan dan tautan ke perangkat lunak berbahaya, mereka memindai lingkungan untuk mengidentifikasi kerentanan perangkat lunak baru, lingkungan baru yang populer di kalangan pengguna Internet, dan vektor serangan baru. Di antara bentuk penipuan yang lebih cerdik dalam beberapa tahun terakhir adalah ransom ware polisi. Perangkat lunak berbahaya ini mengunci komputer pengguna hingga denda dibayarkan ke rekening bank online. Lambang dan merek lembaga penegak hukum yang sah direproduksi untuk meyakinkan pengguna bahwa mereka berurusan dengan polisi asli di negara asal mereka, kesan yang diperkuat dengan terjemahan pemberitahuan ke dalam bahasa yang sesuai. Pengguna diberi tahu bahwa mereka telah terlibat dalam aktivitas kriminal online, misalnya mengunduh materi yang melecehkan anak atau file audiovisual bajakan.

Dengan mempermainkan ketakutan dan rasa bersalah para korban, kejahatan dunia maya semacam ini terbukti sangat menguntungkan. Komunitas penegak hukum, didukung oleh European Cybercrime Center (EC3) di Europol dan Interpol, membuat kemajuan nyata

melawan kelompok kriminal yang terlibat dalam distribusi ransom ware. Pada bulan Februari 2013, Operasi Ransom, yang dipimpin oleh polisi Spanyol, mengakibatkan 11 penangkapan untuk produksi, pengembangan dan distribusi malware jenis ini, dan penangkapan 10 orang lain yang terlibat dalam sisi keuangan penipuan. Investigasi sedang berlangsung.

Jaringan ribuan komputer yang terinfeksi yang pada dasarnya berfungsi sebagai zombie untuk melakukan serangan pada sistem lain, botnet telah mempercepat industrialisasi Cybercrime lebih dari alat lainnya. Sebelum munculnya botnet, korban kejahatan dunia maya menjadi sasaran satu per satu, membutuhkan waktu dan upaya yang jauh lebih besar dari pihak penjahat. Saat ini, pengiriman spam dan serangan Distributed Denial of Service yang menghentikan situs web pemerintah dan komersial dengan membanjiri lalu lintas Internet sangat bergantung pada botnet untuk kekuatan pemrosesannya. Komputer pribadi, notebook, atau smartphone Anda mungkin telah dieksploitasi dengan cara ini.

Botnet tidak hanya kuat tetapi juga sangat hemat biaya, dengan harga turun menjadi $150 dalam beberapa bulan terakhir. Dan seperti halnya bisnis yang sah memindahkan komputasi mereka ke Cloud, kita juga dapat berharap untuk melihat botnet Cloud dalam waktu dekat—entitas yang sangat dinamis yang akan dengan cepat mengubah lokasi, sehingga membutuhkan kerjasama internasional yang tepat waktu dan terpadu untuk dibongkar.

Sementara itu, Internet semakin ditunjuk sebagai infrastruktur penting. Ini juga merupakan teknologi yang diandalkan oleh sebagian besar infrastruktur penting, termasuk catu daya, penyediaan layanan kesehatan, dan komunikasi darurat.

Sebagai warga dunia pada tahun 2013, Anda mungkin dimaafkan jika berpikir bahwa ancaman dari kejahatan dunia maya tidak nyata atau setidaknya dilebih-lebihkan. Sementara statistik yang dikutip di media populer secara rutin merujuk pada jutaan perangkat komputasi yang terinfeksi dan miliaran dolar AS yang hilang melalui intrusi atau penipuan online, dampak langsung dari hal ini jarang dirasakan oleh rata-rata pengguna Internet, yang akan diganti oleh layanan keuangan mereka. penyedia dan mungkin merasa tidak perlu melaporkan kejahatan ke polisi. Berbeda dengan, katakanlah, eksploitasi seksual anak secara online, kejahatan dunia maya hingga saat ini, sebagian besar, tidak menimbulkan kerugian yang signifikan pada korbannya.

Namun, ini kemungkinan akan berubah dalam waktu dekat. Meningkatnya ketergantungan warga yang rentan pada perangkat medis berkemampuan Internet seperti alat pacu jantung, defibrillator dan pompa insulin, dikombinasikan dengan populasi yang menua di banyak bagian dunia, menyoroti pentingnya peningkatan kesadaran dan kebersihan digital untuk anggota masyarakat yang lebih tua. Ini mungkin terdengar seperti fiksi ilmiah, tetapi saya berbicara dari pengalaman. Ayah saya sendiri dipasangi alat pacu jantung berkemampuan nirkabel tetapi tidak tahu konsekuensi potensial dari tidak memperbarui perangkat lunak anti-virusnya. Dan tidak semua orang memiliki kemewahan penyelidik kejahatan dunia maya dalam keluarga mereka.

Penegakan hukum telah sepenuhnya menyadari ancaman dari kejahatan dunia maya selama lebih dari satu dekade, tetapi perlu beberapa waktu bagi kejahatan dunia maya untuk menikmati prioritas dalam hal sumber daya. Di seluruh dunia, kemampuan memerangi kejahatan dunia maya berkembang dengan kecepatan yang sangat berbeda. Ke mana pun saya melakukan perjalanan dalam pekerjaan saya untuk EC3, saya belum pernah mengunjungi

lembaga penegak hukum yang mengklaim memiliki sumber daya yang cukup untuk memerangi ancaman atau untuk secara efektif mengelola beban kerja sebesar sejumlah investigasi yang seringkali memerlukan pemeriksaan terabyte data. Badan-badan lokal dan nasional yang beroperasi dalam isolasi tidak diragukan lagi tidak memanfaatkan sumber daya mereka dengan sebaik-baiknya.

Ketika kita melihat kembali tahun 2013 dan 2014, kita akan melihat tahun-tahun ini sebagai tonggak penting dalam perang melawan kejahatan dunia maya. Pada Januari 2013, EC3 dibuka. Berbasis di Europol di Den Haag, pusat tersebut memberikan dukungan operasional spesialis dan koordinasi intelijen untuk penyelidikan kejahatan dunia maya di 27 negara anggota Uni Eropa dan, pada gilirannya, memanfaatkan kemampuan dan keahlian mereka untuk memberikan tanggapan yang lebih komprehensif dan tepat sasaran terhadap ancaman online.

Pada tahun 2014, Pusat Kejahatan Digital interpol akan beroperasi di Kompleks Global untuk Inovasi di Singapura. Dalam pengembangan kedua pusat tersebut, penekanan kuat ditempatkan pada penyampaian tanggapan kolaboratif yang melibatkan berbagai pemangku kepentingan keamanan siber, termasuk industri, akademisi dan organisasi masyarakat sipil, serta otoritas pemerintah.

EC3, misalnya, telah bermitra dengan International Cyber Security Protection Alliance (ICSPA). Didukung oleh Perdana Menteri Inggris, David Cameron, ini adalah prakarsa yang menyatukan penegakan hukum dan industri keamanan Internet dalam memberikan peningkatan kapasitas global dan pencegahan kejahatan dunia maya. Di bawah naungan ICSPA, EC3 memimpin Proyek 2020 dengan melihat skenario yang mengantisipasi masa depan kejahatan dunia maya dan berupaya mempersiapkan warga, bisnis, dan pemerintah dengan menggunakan materi peningkatan kesadaran yang menarik, seperti film dan animasi. Ketika teknologi berkembang secepat Internet, ada baiknya untuk selangkah lebih maju.

Tidak ada yang bisa memprediksi masa depan secara akurat, tetapi kami cukup yakin bahwa beberapa teknologi yang muncul akan lebih menonjol pada tahun 2020. Augmented reality sudah terlihat dalam bentuk aplikasi smartphone yang memberikan informasi online tentang lokasi fisik pengguna: ulasan khusus untuk restoran dan aplikasi lokal yang memetakan langit malam di mana pun Anda berada, tetapi tampilan yang dipasang di kepala seperti Google Glass diatur untuk mengintegrasikan konten tambahan ini secara lebih lengkap ke dalam pengalaman kami di dunia offline.

Internet of Things adalah frasa yang sering digunakan untuk menggambarkan penggabungan konektivitas Internet ke dalam sejumlah besar perangkat yang sebelumnya tidak terhubung, seperti peralatan rumah tangga dan pakaian. Dikombinasikan dengan peningkatan lebih lanjut dalam penandaan Identifikasi Frekuensi Radio, proliferasi global sensor berkemampuan Internet memiliki potensi untuk memberikan inovasi yang cukup besar dalam rantai pasokan dan distribusi, sementara munculnya pencetakan 3-D mungkin menjadi katalis untuk model manufaktur baru.

Tak satu pun dari teknologi ini akan beroperasi secara terpisah; sebaliknya, mereka akan menjadi bagian dari satu ekosistem. Tambahkan ke teknologi rumah pintar ini wawasan yang dapat diperoleh dari data besar dan cerdas, dan kemunculan realitas virtual yang telah lama ditunggu-tunggu dalam bentuk teknologi kehadiran jarak jauh seperti beaming, dan

terbukti bahwa lebih banyak data akan dihasilkan oleh semua dari kita, sepanjang waktu. Ini akan terus menarik bagi penjahat dunia maya, yang membutuhkan perlindungan yang ditingkatkan oleh penyedia layanan dan bahkan tingkat kerja sama internasional yang lebih besar oleh mereka yang bertanggung jawab untuk menyelidiki pelanggaran, dan meminta pertanggungjawaban penjahat dunia maya.

Perundang-undangan di seluruh dunia tidak hanya perlu mengejar tetapi juga mengimbangi penyalahgunaan teknologi yang muncul secara kriminal. Sekarang ada risiko nyata bahwa, tanpa harmonisasi, negara-negara dengan tingkat keamanan siber yang lebih rendah, undang-undang kejahatan siber yang lebih lemah, dan kemampuan penegakan hukum yang berkurang akan menjadi tempat berlindung yang aman bagi penjahat siber selama bertahun-tahun yang akan datang.

Kerja sama internasional sudah penting untuk berhasil menyelidiki dan menuntut kejahatan dunia maya. Namun, kita juga perlu berpikir lebih cerdas, di luar praktik peradilan pidana tradisional dalam menangkap, menuntut, dan menghukum individu. Langkah-langkah gangguan dan pencegahan yang efektif, dan akan terus, mungkin dilakukan. Organisasi internasional seperti Europol, Interpol, dan Perserikatan Bangsa-Bangsa adalah pengganda kekuatan dalam penyampaian inisiatif multi-sektor yang efektif untuk membongkar botnet, mengurangi keuntungan ekonomi bawah tanah digital, dan secara aktif melibatkan warga dalam perlindungan terhadap serangan.

Perang melawan kejahatan dunia maya juga membutuhkan pusat informasi khusus dan koordinasi intelijen. Sangat sering hanya di tingkat internasional para analis dapat memperoleh gambaran yang akurat tentang tingkat dan bahaya kegiatan kelompok penjahat dunia maya. Komunitas penegak hukum dan keamanan, misalnya, membutuhkan organisasi seperti Europol, Interpol, Kantor PBB untuk Narkoba dan Kejahatan, dan Lembaga Penelitian Kejahatan dan Keadilan Antar-Kawasan PBB untuk membantu mereka memahami ancaman, dan membuat hubungan penting antara pelanggaran di sering sangat berbeda bagian dunia.

Selama beberapa tahun, komunitas internasional telah menggambarkan kejahatan dunia maya sebagai tanpa batas. Sekarang saatnya untuk berjalan dan memberikan tanggapan yang benar-benar terkoordinasi yang tidak hanya tepat waktu tetapi juga responsif terhadap perubahan teknologi Internet. Dengan bekerja sama dengan tujuan bersama untuk Internet yang lebih aman, kami akan memastikan tidak hanya bahwa kami menghadapi ancaman saat ini seefektif mungkin, tetapi kami juga akan fit untuk masa depan.

17.7 PERSERIKATAN BANGSA-BANGSA DAN KEJAHATAN DUNIA MAYA

Perserikatan Bangsa-Bangsa telah di Majelis Umum, Resolusi 65/230, memprakarsai studi tentang masalah kejahatan dunia maya, untuk mengadakan kelompok ahli antar pemerintah terbuka untuk melakukan studi komprehensif tentang masalah kejahatan dunia maya serta tanggapan mereka terhadap dia. Kelompok studi ini diselenggarakan oleh UNODC di Wina,

«dengan maksud untuk memeriksa pilihan untuk memperkuat yang ada dan untuk mengusulkan hukum nasional dan internasional baru atau tanggapan lain terhadap kejahatan dunia maya».

Kelompok ahli mengadakan Sesi Pertama di Wina, Januari 2011. Kuesioner pada Februari 2012 dikirim ke semua Negara Anggota Perserikatan Bangsa-Bangsa, sektor swasta, IGO dan akademisi. Lokakarya regional juga diselenggarakan. Sesi Kedua diadakan di Wina pada 25-28 Februari 2013. Rancangan dan rekomendasi studi dibahas, dan Sidang memutuskan langkah ke depan.

Majelis Umum

Majelis Umum pada tahun 2010 mengadopsi Resolusi 65/230 yang awalnya didasarkan pada Deklarasi Salvador Pasal 42. Rancangan Resolusi oleh Komisi Pencegahan Kejahatan dan Peradilan Pidana dalam Pasal 8 didasarkan pada Deklarasi Salvador Pasal 42 (2010). Resolusi tersebut mengajukan usulan untuk menetapkan sebagai berikut:

Sebuah kelompok ahli antar pemerintah terbuka untuk melakukan studi komprehensif tentang masalah kejahatan dunia maya dan tanggapannya oleh Negara-negara Anggota, komunitas internasional dan sektor swasta, termasuk pertukaran informasi tentang undang-undang nasional, praktik terbaik, bantuan teknis dan internasional kerjasama, dengan maksud untuk mengkaji pilihan untuk memperkuat yang ada dan untuk mengusulkan hukum nasional dan internasional baru atau tanggapan lain terhadap kejahatan dunia maya.

Resolusi tersebut diadopsi oleh Komisi, dan kemudian oleh Majelis Umum PBB dalam Resolusi 65/230. Resolusi tentang pemberantasan penyalahgunaan teknologi informasi diadopsi oleh Majelis Umum pada 4 Desember 2000 Resolusi 55/63, termasuk sebagai berikut: "(a) Negara harus memastikan bahwa undang-undang dan praktik mereka menghilangkan tempat berlindung yang aman bagi mereka yang menyalahgunakan teknologi informasi secara kriminal.

(d) Sistem hukum harus melindungi kerahasiaan, integritas, dan ketersediaan data dan sistem komputer dari gangguan yang tidak sah dan memastikan bahwa penyalahgunaan kriminal dihukum."

Resolusi 56/121 diadopsi pada 19 Desember 2001, termasuk rekomendasi tentang pencegahan dan pemberantasan penyalahgunaan teknologi informasi.

Kantor PBB untuk Narkoba dan Kejahatan (UNODC): Kongres PBB tentang Pencegahan Kejahatan dan Peradilan Pidana telah melihat masalah teknis dan penegakan pidana penyalahgunaan komputer untuk setidaknya empat Kongres terakhir. Perserikatan Bangsa-Bangsa mengadopsi pada tahun 1990 sebuah resolusi tentang undang-undang kejahatan komputer di Kongres PBB ke-8 tentang Pencegahan Kejahatan dan Perlakuan terhadap Pelanggar di Havana, Kuba. Kongres 12 terakhir di Salvador, Brasil, (2010) berfokus pada isu-isu kejahatan dunia maya beberapa peristiwa. Laporan Kongres dan makalah latar belakang keduanya tersedia dari Kantor PBB untuk Narkoba dan Kejahatan.

17.8 UPAYA PBB UNTUK MELINDUNGI ANAK DARI KEJAHATAN DUNIA MAYA

Pada Mei 2011, Komisi PBB untuk Pencegahan Kejahatan dan Peradilan Pidana menerbitkan laporan dari pertemuan kedua puluhnya di Wina, dengan fokus pada masalah yang berkembang dari kejahatan dunia maya terhadap anak-anak. CCPCJ, anak perusahaan Dewan Ekonomi dan Sosial dan badan pengatur Kantor PBB untuk Narkoba dan Kejahatan, melakukan tindakan internasional untuk memerangi kejahatan nasional dan transnasional, mempromosikan peran hukum pidana untuk mencegah perdagangan ilegal sumber daya

alam, kejahatan pencegahan di daerah perkotaan, dan meningkatkan efisiensi dan keadilan sistem peradilan pidana. Wawasan ini berfokus pada diskusi tematik pertemuan kedua puluh: Melindungi anak di era digital: penyalahgunaan teknologi dalam penyalahgunaan dan eksploitasi anak.€ •

Kejahatan Virtual, Korban Nyata: Direktur Eksekutif UNODC, Yury Fedotov, membuka pertemuan kedua puluh CCPCJ dengan membingkai ruang lingkup kejahatan dunia maya terhadap anak-anak. Dia menekankan bahwa dengan hampir dua miliar pengguna internet di seluruh dunia, ada â€ peluang [bagi penjahat] untuk menjebak korban baru, termasuk anak-anak. Secara khusus, teknologi informasi baru disalahgunakan untuk melakukan kejahatan seperti: (a) eksploitasi anak; (b) produksi, distribusi, dan kepemilikan pornografi anak; (c) paparan konten berbahaya; (d) perawatan, pelecehan, dan pelecehan seksual; dan (e) perundungan siber.

Teknologi terbaru memudahkan para penjahat untuk menghubungi anak-anak dengan cara yang sebelumnya tidak mungkin dilakukan. Anak-anak sangat rentan terhadap eksploitasi predator online karena mereka sangat bergantung pada situs jejaring untuk interaksi sosial. Pelaku menggunakan identitas palsu di ruang obrolan untuk memikat korban ke pertemuan fisik, sehingga menghubungkan dunia cyber dan kejahatan fisik. Ketika ini terjadi, kejahatan virtual seringkali mengarah pada bentuk-bentuk tradisional pelecehan dan eksploitasi anak seperti perdagangan manusia dan wisata seks. Para korban eksploitasi online harus hidup dengan pelecehan mereka selama sisa hidup mereka. Dipercaya secara luas bahwa paparan konten tertentu dan kontak yang mudah dengan penjahat online dapat mempengaruhi perkembangan integral anak-anak. Dan begitu informasi dan gambar online, mereka tetap online selamanya dan tersedia untuk semakin banyak orang. Para ahli pada pertemuan kedua puluh CCPCJ mengingatkan para delegasi bahwa gambar pelecehan online adalah hasil dari kejahatan fisik yang sebenarnya.

Kejahatan tanpa Batas: Perusahaan kriminal mendapatkan keuntungan dari anonimitas relatif yang disediakan internet. Otoritas penegak hukum berjuang untuk menemukan pelanggar karena kemampuan untuk menyembunyikan identitas online dan melindungi kegiatan yang melanggar hukum dengan program keamanan. Anonimitas ini diperparah oleh penggunaan strategis penyedia layanan internet di berbagai yurisdiksi. Ketika pelaku mencurigai bahwa penegak hukum di satu yurisdiksi melacak aktivitasnya, dia hanya perlu memindahkan perusahaan kriminal ke ISP di luar jangkauan otoritas tersebut.

Akibatnya, tindakan cepat diperlukan untuk menghubungkan eksploitasi dunia maya anak-anak kepada pengguna sebelum mereka dapat mentransfer ke keamanan relatif dari ISP yang berbeda. Penjahat juga menggagalkan penegakan hukum dengan mengembangkan cara-cara baru untuk melanjutkan kesalahan mereka. Situs web komersial pernah menjadi sumber utama gambar eksploitatif online anak-anak, di mana individu membayar biaya untuk mengakses konten situs. Kelompok-kelompok ini sekarang bergerak menuju jejaring sosial yang lebih kecil, situs berbagi gambar, platform hosting gratis, dan situs web yang diretas. Jaringan peer-to-peer yang kurang formal tidak meninggalkan jejak uang, sehingga lebih sulit bagi penegak hukum untuk mengidentifikasi pelaku online.

17.9 KERJASAMA EKONOMI ASIA-PASIFIK DAN KEJAHATAN CYBER

Di kawasan Asia-Pasifik, APEC mengoordinasikan 21 negara anggotanya untuk mempromosikan keamanan siber dan untuk mengatasi risiko yang ditimbulkan oleh kejahatan siber. APEC telah melakukan proyek pengembangan kapasitas tentang kejahatan dunia maya untuk ekonomi anggota dalam kaitannya dengan struktur hukum dan kemampuan investigasi, di mana ekonomi APEC yang maju mendukung ekonomi anggota lainnya dalam melatih personel legislatif dan investigasi.

Setelah serangan 9/11 di AS, para Pemimpin APEC mengeluarkan Pernyataan tentang Kontra-Terorisme, mengutuk serangan teroris dan menganggapnya mendesak untuk memperkuat kolaborasi di berbagai lapisan untuk memerangi terorisme. Para Pemimpin menyerukan untuk memperkuat kegiatan APEC untuk melindungi infrastruktur penting.

Menteri Telekomunikasi dan Informasi ekonomi APEC mengeluarkan Pernyataan tentang Keamanan Infrastruktur Informasi dan Komunikasi dan Program Aksi pada tahun 2002, mendukung langkah-langkah yang diambil oleh anggota untuk memerangi penyalahgunaan informasi. Pertemuan Pejabat Senior telah membuat rekomendasi yang menetapkan enam bidang yang dapat berfungsi sebagai dasar bagi upaya APEC untuk pencegahan kejahatan dunia maya, yang terdiri dari pengembangan hukum, pembagian dan kerja sama informasi, keamanan dan pedoman teknis, kesadaran publik, pelatihan dan pendidikan, dan nirkabel. keamanan.Para Menteri dan Pemimpin APEC telah membuat komitmen untuk "berusaha untuk memberlakukan seperangkat undang-undang yang komprehensif terkait dengan keamanan dunia maya dan kejahatan dunia maya yang konsisten dengan ketentuan instrumen hukum internasional, termasuk Resolusi Majelis Umum PBB 55/63 dan Konvensi tentang Cybercrime pada Oktober 2003."

Menanggapi panggilan dari para pemimpin ini, survei undang-undang dilakukan dan ringkasan dibuat dari tanggapan dari ekonomi anggota yang diterima pada tahun 2003. Ekonomi mengusulkan proyek terkait dalam kelompok tugas keamanan informasi. Misalnya, A.S. mengusulkan sebuah proyek di E-Security Task Group dari Telecommunications and Information Working Group. Tahap pertama dari proyek ini adalah pertemuan para ahli kejahatan dunia maya dari seluruh wilayah. Pertemuan tersebut diadakan pada tanggal 21-25 Juli 2003 di Bangkok, Thailand, dan dihadiri oleh lebih dari 120 delegasi dari 17 negara. Tujuan pertemuan tersebut adalah untuk membantu perekonomian mengembangkan kerangka hukum yang diperlukan; untuk mempromosikan pengembangan kapasitas penegakan hukum; serta memperkuat kerja sama antara sektor swasta dan publik dalam mengatasi ancaman kejahatan dunia maya. Dalam konferensi tersebut, para ahli yang hadir sepakat bahwa setiap perekonomian membutuhkan kerangka hukum termasuk hukum substantif dan prosedural, serta hukum dan kebijakan kerjasama antar ekonomi. Mereka menegaskan peran instrumen internasional, khususnya Konvensi Cybercrime. Mereka juga menekankan kerja sama yurisdiksi, konstruksi penegakan hukum, dan peningkatan kapasitas para penyelidik.

Pada tahun 2005, Pertemuan Menteri APEC keenam tentang Industri Telekomunikasi dan Informasi mengesahkan Deklarasi Lima, "mendorong semua ekonomi untuk mempelajari Konvensi Kejahatan Dunia Maya (2001) dan berusaha untuk memberlakukan seperangkat undang-undang yang komprehensif terkait dengan keamanan dunia maya dan kejahatan dunia maya yang konsisten dengan instrumen hukum internasional, termasuk Resolusi Majelis

Umum PBB 55/63 (2000) dan Konvensi Kejahatan Dunia Maya (2001). Namun, karena perbedaan besar antara ekonomi anggota dalam APEC, perkembangan menuju instrumen hukum terpadu belum terlalu memuaskan. Meskipun beberapa negara telah mengklaim bahwa undang-undang mereka telah sepenuhnya konsisten dengan Konvensi, dan beberapa negara lain mengambil tindakan untuk menerapkan ketentuan yang serupa dengan Konvensi, banyak negara lain memiliki sistem hukum yang sangat berbeda atau tidak memiliki undang-undang yang mengkriminalisasi kejahatan dunia maya.

Upaya masih harus dilakukan di forum APEC untuk mengatasi kejahatan dunia maya. AS mengusulkan Proyek Pembangunan Kapasitas Cybercrime Hakim dan Jaksa pada tahun 2006 untuk mengembangkan kurikulum yang dirancang oleh para ahli pemerintah dan sektor swasta; menerjemahkan kurikulum ke dalam bahasa domestik; dan melatih pelatih (hakim dan jaksa).

17.10 UNI EROPA DAN KEJAHATAN CYBER

Uni Eropa mengambil serangkaian tindakan untuk mengatasi kejahatan dunia maya dengan mendorong penegakan hukum yang terkoordinasi dan kebijakan harmonisasi hukum. Kebebasan sipil juga telah menjadi fokus di bidang anti-kejahatan siber. Pada tahun 1995, Parlemen Eropa dan Dewan mengesahkan Arahan 95/46/EC tanggal 24 Oktober 1995 tentang perlindungan Individu sehubungan dengan Pemrosesan Data Pribadi dan Pergerakan Data Tersebut. Bagian VIII Arahan ini secara khusus mengatur kerahasiaan dan keamanan pemrosesan data pribadi. Arahan ini berlaku untuk perlindungan orang perseorangan (Pasal 2(a)). Cakupan Instruksi terbatas pada pemrosesan data pribadi seluruhnya atau sebagian dengan cara otomatis (Pasal 3-1). Arahan tersebut mensyaratkan bahwa langkah-langkah teknis dan organisasi yang sesuai harus diterapkan untuk melindungi data pribadi dari perusakan ilegal, perubahan, akses, dan bentuk pemrosesan ilegal lainnya (Pasal 17-1). Arahan tersebut mengharuskan Negara-negara Anggota untuk memberikan pemulihan administratif dan yudisial bagi korban (Pasal 22), dan mengatur tanggung jawab kompensasi (Pasal 23) dan sanksi terhadap (Pasal 24) pelanggar.

Pada tahun 1997, Parlemen Eropa dan Dewan mengesahkan Arahan 97/66/EC tanggal 15 Desember 1997 tentang Pemrosesan Data Pribadi dan Perlindungan Privasi di Sektor Telekomunikasi. Arahan tersebut bertujuan untuk memajukan perlindungan yang diterapkan dalam Arahan 95/46/EC, dan menyediakan harmonisasi ketentuan negara-negara anggota untuk mencapai tingkat perlindungan yang setara (Pasal 1-1). Arahan tersebut memperluas perlindungan kepentingan yang sah kepada badan hukum (Pasal 1-2).

Lingkup penerapan Arahan ini terbatas pada pemrosesan data pribadi yang berkaitan dengan penyediaan layanan telekomunikasi yang tersedia untuk umum dalam jaringan telekomunikasi publik; khususnya melalui ISDN (Jaringan Digital Layanan Terpadu), dan jaringan seluler digital publik (Pasal 3-1). Karena Directive 95/46/EC berkaitan dengan sistem pemrosesan otomatis, Directive 97/66/EC telah menekankan keterkaitan dengan jaringan telekomunikasi. Arahan tersebut memberikan persyaratan yang secara langsung ditujukan pada penyedia layanan (tetapi bukan negara anggota) "untuk mengambil langkah-langkah teknis dan organisasional yang sesuai untuk menjaga keamanan layanannya." (Pasal 4-1). Arahan tersebut mengharuskan Negara-negara Anggota untuk menerapkan peraturan yang

memastikan kerahasiaan komunikasi, melarang mendengarkan, menyadap, menyimpan atau jenis intersepsi atau pengawasan komunikasi lainnya oleh orang dan badan hukum yang tidak berwenang (Pasal 5). Directive membatasi komunikasi yang tidak diminta (Pasal 12), yang mencakup sistem panggilan otomatis atau mesin faksimili, tetapi tidak email.

Pada tanggal 27 November 2001, sebuah sesi pleno berlangsung di Brussel dari Forum Uni Eropa tentang Kejahatan Dunia Maya, yang diselenggarakan oleh EC, dan di mana diskusi utama adalah tentang penyimpanan data lalu lintas (Forum Uni Eropa tentang Kejahatan Dunia Maya, 2001).

Pada bulan April 2002, Komisi Komunitas Eropa mengajukan proposal untuk Keputusan Kerangka Kerja Dewan tentang Serangan terhadap sistem informasi, dan proposal ini merupakan kasus Keputusan 24 Februari 2005. Keputusan Kerangka tersebut mengkriminalisasi pelanggaran akses ilegal ke sistem informasi (Pasal 2), gangguan sistem ilegal (Pasal 3), gangguan data ilegal (Pasal 4), dan penghasutan, membantu dan bersekongkol dengan pelanggaran ini atau mencoba melakukannya (Pasal 5). Keputusan Kerangka Kerja hanya menangani serangan melalui akses tidak sah ke atau gangguan pada sistem informasi atau data. Menurut Keputusan tersebut, akses ilegal hanya dapat dibentuk ketika kegiatan ilegal ditargetkan secara sengaja terhadap "sistem informasi dengan langkah-langkah perlindungan khusus dan [serangan] harus untuk keuntungan ekonomi." (Pasal 2)

Komisi lebih lanjut mempertimbangkan kemungkinan masa depan "tindakan perlindungan khusus" (Usulan untuk Keputusan Kerangka Dewan tentang Serangan terhadap sistem informasi) ke jaringan broadband, dengan mengatakan bahwa, "hukum pidana perlu mencakup akses tidak sah ke sistem mereka meskipun mungkin ada tidak menjadi perlindungan teknis yang memadai untuk sistem mereka." (ibid.) Jadi, mengenai gangguan terhadap sistem informasi, hal itu didasari oleh "penghambatan" atau "pengganggguan" yang serius terhadap fungsi sistem informasi dengan "memasukkan, mentransmisikan, merusak, menghapus, memperburuk, mengubah, menekan atau membuat komputer tidak dapat diakses. data" (Pasal 3).

Kerangka Keputusan ini tidak menentukan hukuman untuk akses ilegal ke sistem informasi dan hasutan, membantu dan bersekongkol dan mencoba pelanggaran ini, tetapi mengharuskan negara-negara anggota untuk mengambil langkah-langkah yang diperlukan untuk memastikan bahwa mereka dapat dihukum dengan hukuman pidana yang efektif, proporsional dan menghalangi (Framework Putusan, Pasal 6.1). Keputusan tersebut menetapkan hukuman untuk gangguan sistem ilegal dan gangguan data ilegal yang dapat dihukum dengan hukuman pidana paling sedikit satu sampai tiga tahun penjara (Pasal 6.2). Adapun “keadaan yang memberatkan”, pelaku diancam dengan pidana penjara paling singkat dua sampai lima tahun (Pasal 7.1). Keadaan yang memberatkan ini termasuk serangan terorganisir, dan serangan yang "menyebabkan kerusakan serius atau mempengaruhi kepentingan penting" (Pasal 7.2).

Organisasi kriminal didefinisikan sebagai "asosiasi terstruktur, didirikan selama periode waktu, dari dua orang atau lebih, bertindak secara bersama-sama dengan maksud untuk melakukan pelanggaran." Perlu dicatat bahwa hal-hal yang disebutkan dalam Kerangka Keputusan juga dapat ditemukan dalam Konvensi Cybercrime. Setelah revisi undang-undang

yang disyaratkan oleh Konvensi, hukum nasional (Finlandia) juga akan memenuhi tuntutan Keputusan Kerangka Kerja.

17.11 RINGKASAN

Peran organisasi internasional sangat krusial dan penting untuk memerangi cyber terrorism dan cyber crime secara global. Dalam unit ini konsep penting INTERPOL dan kejahatan dunia maya, Biro Investigasi Federal (FBI) dan kejahatan dunia maya, memerangi industrialisasi kejahatan dunia maya, PBB dan kejahatan dunia maya, upaya PBB untuk melindungi anak-anak dari kejahatan dunia maya, Kerjasama Ekonomi Asia-Pasifik dan kejahatan siber dan Uni Eropa dan Kejahatan Siber dibahas panjang lebar untuk memahami berbagai isu terkait kejahatan siber di seluruh dunia.

17.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)
- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Authorpress)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang tepat dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

17.13 PERIKSA KEMAJUAN ANDA

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a) Pada tahun 2011, setidaknya 2,3 miliar orang, setara dengan lebih dari sepertiga penduduk, memiliki akses ke internet.
b) Kejahatan dunia maya adalah area kejahatan yang berkembang pesat.
c) Cybercrime mencakup serangan terhadap perangkat keras dan perangkat lunak komputer.
d) Perundang-undangan di seluruh dunia tidak hanya perlu mengejar tetapi juga mengimbangi penyalahgunaan teknologi yang muncul secara kriminal.
e) Di Kawasan Asia-Pasifik, APEC mengoordinasikan 21 negara anggota untuk mempromosikan keamanan dunia maya dan untuk mengatasi risiko yang ditimbulkan oleh kejahatan dunia maya.‖

B. Isi Bagian yang Kosong:

I. Kejahatan dunia maya mencakup penyalahgunaan terutama …… dalam bentuk 'perawatan' atau 'eksploitasi'.
II. Bisnis cyberciminal adalah……
III. Di ……, pusat Kejahatan Digital baru INTERPOL akan beroperasi sebagai kompleks global untuk inovasi Singapura.
IV. ISPA artinya…..
V. Majelis Umum USN …memulai studi tentang masalah kejahatan dunia maya.

17.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. Orang Muda
2. Terus Berinovasi
3. 2014
4. Aliansi Perlindungan Keamanan Siber Internasional
5. Resolusi 65/230

17.15 PERTANYAAN TERMINAL

1. Membahas INTERPOL dan kejahatan dunia maya.
2. Membahas secara detail FBI dan cyber crime.
3. Membahas PBB dan kejahatan dunia maya.
4. Apa upaya PBB dalam melindungi anak dari kejahatan dunia maya?
5. Membahas secara rinci Kerjasama Ekonomi Asia-Pasifik dan kejahatan dunia maya.

BAB 18
STUDI KASUS DAN KEJAHATAN CYBER

Tujuan

Setelah melalui unit ini, Anda seharusnya dapat:

- Memahami Kejahatan Cyber melalui berbagai Studi Kasus Internasional
- Memahami Kejahatan Cyber melalui berbagai Studi Kasus India
- Memahami masalah teknis dan hukum terkait Studi Kasus

18.1 PENGANTAR

McAfee dan CSIS: Menghentikan Kejahatan Dunia Maya Dapat Berdampak Positif pada Perekonomian Dunia (Dampak Ekonomi Kejahatan Dunia Maya Diperkirakan mencapai Rp 6.675.000 miliar di Seluruh Dunia, dan antara 15% dan 20% dari nilai yang diciptakan oleh Internet)=SANTA CLARA, California — 9 Juni 2014 — A laporan baru dari Center for Strategic and International Studies (CSIS) dan disponsori oleh McAfee, bagian dari Intel Security, menunjukkan dampak signifikan kejahatan dunia maya terhadap ekonomi di seluruh dunia. . Laporan, "Kerugian bersih – memperkirakan biaya global kejahatan dunia maya," menyimpulkan bahwa kejahatan dunia maya merugikan bisnis sekitar Rp 6.000.000 miliar di seluruh dunia, dengan dampak pada sekitar 200.000 pekerjaan di AS, dan 150.000 pekerjaan di UE.

Biaya paling penting dari kejahatan dunia maya berasal dari kerusakannya terhadap kinerja perusahaan dan ekonomi nasional. Kejahatan dunia maya merusak perdagangan, daya saing, inovasi, dan pertumbuhan ekonomi global. Studi memperkirakan bahwa ekonomi Internet setiap tahun menghasilkan antara Rp 30.000 triliun dan Rp 45.000 triliun, bagian dari ekonomi global yang diperkirakan akan tumbuh pesat. Berdasarkan perkiraan CSIS, kejahatan dunia maya mengekstraksi antara 15% dan 20% dari nilai yang diciptakan oleh Internet. Efek kejahatan dunia maya pada kekayaan intelektual (IP) sangat merusak, dan negara-negara di mana penciptaan IP dan industri intensif IP penting untuk penciptaan kekayaan kehilangan lebih banyak dalam perdagangan, pekerjaan, dan pendapatan dari kejahatan dunia maya daripada negara-negara yang lebih bergantung pada pertanian atau industri manufaktur tingkat rendah , laporan itu ditemukan. Dengan demikian, negara-negara berpenghasilan tinggi kehilangan lebih banyak persen dari PDB daripada negara-negara berpenghasilan rendah – mungkin rata-rata sebanyak 0,9 persen.

"Kejahatan dunia maya adalah pajak atas inovasi dan memperlambat laju inovasi global dengan mengurangi tingkat pengembalian inovator dan investor," kata Jim Lewis dari CSIS. "Untuk negara maju, kejahatan dunia maya memiliki implikasi serius terhadap lapangan kerja. Efek kejahatan dunia maya adalah mengalihkan pekerjaan dari pekerjaan yang menciptakan nilai paling tinggi. Bahkan perubahan kecil dalam PDB dapat mempengaruhi lapangan kerja". Dampak Ekonomi pada Bisnis dan Konsumen Peneliti CSIS menemukan bahwa Amerika Serikat memberi tahu 3.000 perusahaan pada tahun 2013 bahwa mereka telah diretas, dengan pengecer memimpin sebagai target favorit para peretas. Di Inggris, pengecer dilaporkan kehilangan lebih dari Rp 12.750.000 juta karena peretas. Pejabat

Australia melaporkan bahwa serangan skala besar telah terjadi terhadap maskapai penerbangan, jaringan hotel dan perusahaan jasa keuangan, yang menelan biaya sekitar Rp 1.500.000 juta. Dengan perlindungan yang tepat, kerugian ini dapat dihindari.

Laporan tersebut menemukan bahwa kerugian global yang terkait dengan pelanggaran "Informasi pribadi" dapat mencapai Rp 2.400.000 miliar. Empat puluh juta orang di AS, sekitar 15 persen dari populasi, informasi pribadi mereka dicuri oleh peretas. Studi ini melacak pelanggaran profil tinggi di seluruh dunia: 54 juta di Turki; 20 juta di Korea; 16 juta di Jerman dan lebih dari 20 juta di Cina.

Bagian dari kerugian dari kejahatan dunia maya berhubungan langsung dengan apa yang oleh para ahli disebut "biaya pemulihan" atau pembersihan digital dan elektronik yang harus terjadi setelah serangan terjadi. Laporan McAfee-CSIS menemukan bahwa sementara penjahat tidak akan dapat memonetisasi semua informasi yang mereka curi, korban mereka harus menghabiskan sumber daya yang signifikan seolah-olah mereka bisa.

Di Italia, misalnya, kerugian peretasan yang sebenarnya mencapai Rp 13.125.000 juta, tetapi pemulihan, atau biaya pembersihan, mencapai Rp 127.500 miliar. Dengan kata lain, mungkin ada peningkatan sepuluh kali lipat antara kerugian aktual yang secara langsung dikaitkan dengan peretas dan perusahaan pemulihan yang harus diterapkan setelah serangan tersebut. Beralih dari Kerugian ke Potensi Keuntungan Ekonomi Pemerintah mulai serius, upaya sistematis untuk mengumpulkan dan mempublikasikan data tentang kejahatan dunia maya untuk membantu negara dan perusahaan membuat pilihan yang lebih baik tentang risiko dan kebijakan. Peningkatan kerjasama internasional, serta kemitraan publik/swasta juga mulai menunjukkan hasil nyata dalam mengurangi kejahatan dunia maya. Pekan lalu, 11 negara mengumumkan penghapusan jaringan kejahatan yang terkait dengan kap Game Over Zeus.

"Jelas bahwa ada dampak ekonomi nyata yang nyata terkait dengan penghentian kejahatan dunia maya" kata Scott Montgomery, chief technology officer, sektor publik di McAfee. "Selama bertahun-tahun, kejahatan dunia maya telah menjadi industri yang berkembang, tetapi itu dapat diubah, dengan kolaborasi yang lebih besar antar negara, dan peningkatan kemitraan publik-swasta. Teknologi ini ada untuk menjaga informasi keuangan dan kekayaan intelektual tetap aman, dan ketika kami melakukannya, kami menciptakan peluang untuk pertumbuhan ekonomi yang positif dan penciptaan lapangan kerja di seluruh dunia."

18.2 KEJAHATAN CYBER DI INGGRIS-STUDI KASUS

Kejahatan dunia maya di Inggris – studi kasus

Untuk mengontekstualisasikan efek kejahatan siber, menarik untuk mempertimbangkan data yang tersedia untuk negara seperti Inggris. Ini adalah salah satu negara dengan tingkat penetrasi teknologi tertinggi. Data yang dipublikasikan dalam studi terbaru yang dilakukan oleh pakar keamanan siber di University of Kent lebih mengejutkan. Lebih dari 9 juta orang dewasa di Inggris telah diretas akun online, dan 8% dari netizen Inggris terungkap telah menjadi korban kejahatan dunia maya pada tahun lalu. 2,3% dari populasi melaporkan kehilangan lebih dari £ 10.000 untuk penipu online.

Kejahatan utama yang diderita oleh pengguna online Inggris adalah peretasan akun layanan web mereka. Itu termasuk perbankan online, email, dan media sosial. Dalam hampir 33% kasus, pelanggaran itu diulangi.

Pada tahun 2011, pemerintah Inggris mendokumentasikan dalam sebuah laporan resmi bahwa biaya keseluruhan ekonomi kejahatan dunia maya adalah Rp 270.000 miliar per tahun. Pencurian identitas adalah kejahatan yang paling umum, terhitung Rp 17.000 miliar. Itu diikuti oleh penipuan online, dengan Rp 14.000 miliar. Kejahatan dunia maya di Inggris adalah yang paling berbahaya bagi organisasi, bisnis swasta, dan kantor pemerintah, yang menderita spionase dunia maya dan pencurian kekayaan intelektual tingkat tinggi. Media sosial adalah target utama munculnya kejahatan dunia maya di Inggris. Kode berbahaya digunakan oleh geng kriminal untuk mengeksploitasi jaringan sosial untuk penipuan perbankan atau untuk kampanye phishing. Tren baru telah muncul dalam beberapa bulan terakhir. Kode berbahaya yang sama digunakan oleh penjahat untuk meretas akun korban, untuk membuat jejaring sosial palsu 'suka' yang dapat digunakan untuk menghasilkan buzz untuk perusahaan atau individu.

"Suka" palsu dijual dengan lot 1000 per unit, di bawah tanah. RSA memperkirakan bahwa 1000 “pengikut” instagram dapat dibeli seharga Rp 225.000 (Rp 95.000), dan 1000 “Suka” instagram berharga “30 (Rp 190.000). Ini lebih menguntungkan untuk dijual. Pertimbangkan, saat menjual nomor kartu kredit, mereka dijual seharga Rp 90.000 (Rp 38.000) untuk banyak 1000 nomor.

“Tampaknya kejahatan online memiliki dampak yang jelas pada kehidupan rata-rata warga Inggris, dengan akun dan kredensial mereka dikompromikan secara signifikan dan dalam beberapa kasus berkali-kali. Kejahatan dunia maya mungkin belum menyerang sebagian besar publik Inggris, tetapi serangan yang berhasil cenderung menyebabkan kerusakan finansial yang substansial,” kata Dr Julio Hernandez-Castro dan Dr Eerke Boiten, dari Pusat Penelitian Keamanan Siber Interdisipliner Universitas Kent.

Kejahatan dunia maya sebagai layanan

Istilah "serangan sebagai layanan," "Malware sebagai layanan" dan "Penipuan sebagai Layanan" digunakan untuk memenuhi syarat model penjualan di penjahat dunia maya penyihir yang menjual atau menyewakan layanan peretasan dan kode berbahaya rekan mereka, untuk melakukan kegiatan ilegal. Konsepnya revolusioner, pasar gelap menawarkan seluruh infrastruktur untuk layanan malware (misalnya hosting antipeluru atau menyewa mesin yang disusupi milik kap besar), dan layanan outsourcing dan kemitraan, termasuk pengembangan perangkat lunak, layanan peretasan, dan, tentu saja, dukungan pelanggan.

Sebagian besar layanan ini disajikan dalam ekonomi bawah tanah, berdasarkan model biaya berlangganan atau tarif tetap, menjadikannya nyaman dan menarik. Biaya pokok mengatur kegiatan kriminal dibagi antara semua pelanggan. Dengan cara ini, penyedia layanan dapat meningkatkan pendapatan mereka, dan klien mendapat manfaat dari pengurangan pengeluaran yang masuk akal, dengan pengetahuan yang dibutuhkan untuk mengelola bisnis ilegal. Layanan ini dicirikan oleh kemudahan penggunaan dan orientasi pelanggan yang kuat. Mereka biasanya memiliki konsol administrasi dan dasbor yang mudah digunakan untuk mengontrol keuntungan. Difusi paradigma komputasi awan telah membawa banyak keuntungan bagi industri TI, tetapi juga peluang baru bagi penjahat cyber. Istilah

“Attack-as-a-service” sebagai kemampuan organisasi kriminal untuk menawarkan layanan peretasan. Sebagian besar kasus mengeksploitasi arsitektur berbasis cloud.

Penjahat dunia maya menawarkan seluruh botnet dan infrastruktur kontrol, yang dihosting di arsitektur cloud untuk disewakan atau dijual. Mesin yang disusupi dapat digunakan untuk mencuri informasi dari para korban (misalnya kredensial perbankan, informasi sensitif) atau untuk meluncurkan serangan DdoS besar-besaran terhadap target tertentu. Harga untuk serangan terhadap komisi sangat bervariasi. Beberapa layanan benar-benar gratis, seperti berlangganan IMDDOS. Sementara itu, biayanya antara Rp 2.250.000 dan Rp 6.000.000 untuk memecahkan kata sandi email dalam waktu kurang dari 48 jam. Salah satu studi paling menarik yang diusulkan mengenai tawaran kejahatan dunia maya dipresentasikan oleh Fortinet pada Desember 2012. Laporan yang dihasilkan oleh perusahaan keamanan tersebut menjelaskan model "Kejahatan sebagai layanan" secara khusus, memberikan daftar harga terperinci untuk peretasan utama. layanan yang ditawarkan dalam "attacks-as-a-service," dengan beberapa data menarik:

- Layanan konsultasi seperti pengaturan botnet, Rp 5.250.000- Rp 6.000.000
- Layanan infeksi/penyebaran, di bawah Rp 1.500.000 per seribu pemasangan
- Botnet dan sewa, Direct Denial of Service (DdoS), Rp 8.025.000 selama 5 jam sehari selama satu minggu, spam email, Rp 600.000 per 20.000 email, dan spam Web, Rp 30.000 per tiga puluh posting.
- Blackhat Search Engine Optimization (SEO), Rp 1.200.000 untuk 20.000 backlink spam.
- Layanan penukaran uang dan bagal antar Operator, komisi 25%.
- Pemecahan CAPTCHA, Rp 15.000 per seribu CAPTCHA, dilakukan oleh manusia yang direkrut.
- Modul upgrade Crimeware: Menggunakan modul Zeus sebagai contoh, mereka berkisar dari Rp 7.500.000 sampai Rp 150.000.000.

Hasil di atas disediakan dengan menggunakan modalitas yang berbeda, seperti menyewa, membeli atau menyewa untuk menanggapi kebutuhan klien. Tidak diragukan lagi, meskipun istilah berbeda diadopsi untuk menggambarkan praktik serupa, model di belakang mereka tampaknya menang.

Tren dan perkiraan

Teknologi seperti seluler dan jejaring sosial semakin terancam oleh penjahat dunia maya. Mereka "mengadaptasi" metode serangan Konsolidasi ke platform tersebut, dan mendefinisikan strategi ofensif baru. “Proliferasi perangkat seluler akan mengarah pada penguatan penyalahgunaan berdasarkan pengetahuan/vektor serangan yang menargetkan media sosial.” Menurut pakar keamanan dan perusahaan keamanan, penawaran pasar gelap mendukung pertumbuhan ancaman dunia maya dalam ekosistem kejahatan dunia maya.

Seperti yang dilaporkan dalam ENISA Threat Landscape, Mid Year 2013, ancaman utama berikut adalah kandidat untuk mendominasi lanskap kriminal dalam jangka menengah:

- Drive-by-exploit: Serangan berbasis browser masih tetap menjadi ancaman yang paling banyak dilaporkan, dan Java tetap menjadi perangkat lunak yang paling banyak dieksploitasi untuk jenis ancaman ini.
- Worms/Trojan: Malware canggih digunakan oleh penjahat dunia maya dan pemerintah untuk berbagai tujuan, seperti serangan ofensif, spionase dunia maya, dan

penipuan dunia maya yang canggih. Kejahatan dunia maya memanfaatkan malware secara ekstensif, terutama untuk penipuan perbankan. Platform seluler dan situasi jejaring sosial sangat memprihatinkan. Platform tersebut dieksploitasi untuk menyebarkan agen jahat berskala besar.

- Injeksi Kode: Serangan sangat populer terhadap Sistem Manajemen Konten (CMS) web. Karena penggunaannya yang luas, CMS populer merupakan permukaan serangan yang cukup besar yang telah menarik perhatian penjahat dunia maya. Jaringan penyedia layanan cloud semakin banyak digunakan untuk meng-host alat untuk serangan otomatis.
- Botnet, Denial of Services, rogueware/scareware, serangan yang ditargetkan, pencurian identitas, dan keracunan mesin pencari akan terus menjadi ancaman serius bagi komunitas TI.

18.3 KASUS ASIA-PASIFIK YANG DIPILIH

1. Dalam kasus pelanggaran hak cipta, tiga mahasiswa menerima hukuman pidana karena menjalankan situs Web bernama MP3/WMA Land, yang menawarkan lebih dari 1.800 lagu bajakan untuk diunduh. Mengingat usia mereka pada saat itu dan fakta bahwa mereka tidak pernah mendapat untung dari tindakan mereka, pengadilan memberikan hukuman percobaan 18 bulan untuk dua siswa dan denda tambahan sebesar Rp 75.000.000 untuk salah satu dari mereka. Selain itu, satu siswa dan satu peserta ketiga diberikan 200 jam pengabdian masyarakat.
2. Kabarnya, China telah menjadi pengekspor barang palsu dan bajakan terkemuka ke dunia. Industri AS memperkirakan nilai barang palsu di China sebesar Rp 285.000 miliar hingga Rp 360.000 miliar, dengan kerugian bagi perusahaan AS melebihi US$1,8 miliar per tahun. Masalah pembajakan yang parah berasal dari kombinasi faktor budaya, sejarah dan ekonomi dan selanjutnya diperparah oleh penegakan yang tidak konsisten dan lemah oleh pejabat. Situs dan jaringan berbagi file seperti Jelawat dan Kuro juga berkembang pesat. Distributor perangkat lunak P2P mengklaim bahwa berbagi file termasuk dalam pengecualian penggunaan pribadi untuk hak cipta, tetapi Mahkamah Agung PPeople's China Menolak interpretasi ini. Semakin, pemilik hak cipta dan organisasi yang tepat menantang situs Web file-sharing pada klaim pelanggaran hak cipta.
3. Pengadilan Rakyat No 1 Beijing memutuskan pada bulan April 2004 bahwa situs web chinamp3.com melanggar hak IP dari perusahaan hiburan yang berbasis di Hong Kong, Go East Entertainment dan Sony Music Entertainment (Hong Kong), dan memerintahkan situs tersebut untuk membayar US$19.000 dalam kerusakan. Gugatan itu menyangkut distribusi file musik MP3 yang tidak sah. Terdakwa berdalih bahwa dia hanya menyediakan tautan untuk diunduh dan bukan layanan unduhan langsung, dan oleh karena itu tidak bertanggung jawab atas pelanggaran hak IP. Menurut pengamatan, putusan pengadilan mungkin terbukti menjadi perkembangan signifikan di bidang penegakan hak cipta Tiongkok yang baru lahir di era digital.

18.4 KASUS INDIA TERKAIT DENGAN KEJAHATAN CYBER-I

KASUS SERANGAN PARLEMEN: Biro Penelitian dan Pengembangan Polisi di Hyderabad telah menangani beberapa kasus cyber teratas, termasuk menganalisis dan mengambil informasi dari laptop yang ditemukan dari teroris, yang menyerang Parlemen. Laptop yang disita dari kedua teroris yang ditembak mati saat DPR dikepung pada 13 Desember 2001 itu dikirim ke Divisi Forensik Komputer BPRD setelah para ahli komputer di Delhi gagal melacak banyak dari isinya.

Laptop tersebut berisi beberapa barang bukti yang menguatkan motif kedua teroris tersebut, yaitu stiker Kementerian Dalam Negeri yang mereka buat di laptop dan ditempel di mobil duta besar mereka untuk masuk ke Gedung DPR dan kartu identitas palsu yang salah satunya. kedua teroris itu membawa lambang dan segel Pemerintah India.

Lambang (tiga singa) dipindai dengan hati-hati dan stempelnya juga dibuat dengan cermat bersama dengan alamat tempat tinggal Jammu dan Kashmir. Tetapi deteksi yang cermat membuktikan bahwa itu semua dipalsukan dan dibuat di laptop.

Negara Bagian Tamil Nadu Vs Suhas Katti: Kasus Suhas Katti terkenal karena fakta bahwa vonis tersebut berhasil dicapai dalam waktu yang relatif cepat yaitu 7 bulan sejak pengajuan FIR. Menimbang bahwa kasus serupa telah tertunda di negara bagian lain untuk waktu yang lebih lama, penanganan yang efisien dari kasus yang merupakan kasus pertama dari Chennai Cyber Crime Cell akan diadili layak mendapat perhatian khusus.

Kasus terkait postingan pesan cabul, fitnah, dan menjengkelkan tentang wanita cerai di grup pesan yahoo. E-mail juga diteruskan kepada korban untuk informasi oleh terdakwa melalui akun e-mail palsu yang dibukanya atas nama korban. Postingan pesan tersebut mengakibatkan panggilan telepon yang mengganggu ke wanita itu dengan keyakinan bahwa dia meminta. Berdasarkan pengaduan yang dibuat oleh korban pada Februari 2004, Polisi melacak tersangka ke Mumbai dan menangkapnya dalam beberapa hari berikutnya. Terdakwa adalah teman keluarga korban yang dikenal dan dilaporkan tertarik untuk menikahinya. Namun dia menikah dengan orang lain. Pernikahan ini kemudian berakhir dengan perceraian dan terdakwa mulai menghubunginya sekali lagi. Karena keengganannya untuk menikah dengannya, terdakwa melakukan pelecehan melalui Internet.

Pada 24-3-2004 Charge Sheet diajukan u/s 67 dari IT Act 2000, 469 dan 509 IPC sebelum The Hon'ble Addl. CMM Egmore dengan mengutip 18 saksi dan 34 dokumen dan benda material. Hal yang sama diambil pada file di C.C.NO.4680/2004. Di sisi penuntutan 12 saksi diperiksa dan seluruh dokumen ditandai sebagai Barang Bukti. Pembela berargumen bahwa surat-surat yang menyinggung akan diberikan baik oleh mantan suami pelapor atau pelapor sendiri untuk melibatkan terdakwa sebagai terdakwa yang diduga telah menolak permintaan pelapor untuk menikahinya. Lebih lanjut, Penasihat Hukum berargumen bahwa beberapa bukti dokumenter tidak dapat dipertahankan berdasarkan Bagian 65 B dari Undang-Undang Bukti India. Namun, pengadilan mengandalkan saksi ahli dan bukti lain yang diajukan sebelumnya, termasuk saksi pemilik Warnet dan sampai pada kesimpulan bahwa kejahatan itu terbukti secara meyakinkan. Ld. Tambahan Ketua Metropolitan Magistrate, Egmore, menyampaikan putusan pada 11-05-04 sebagai berikut:

" Terdakwa dinyatakan bersalah melakukan pelanggaran berdasarkan pasal 469, 509 IPC dan 67 UU IT 2000 dan terdakwa dinyatakan bersalah dan dihukum karena pelanggaran tersebut

untuk menjalani RI selama 2 tahun berdasarkan 469 IPC dan membayar denda Rs.500 / - dan untuk pelanggaran u/s 509 IPC divonis 1 tahun penjara Sederhana dan membayar denda Rs.500/- dan untuk pelanggaran u/s 67 UU IT 2000 menjalani RI selama 2 tahun dan membayar denda Rs. .4000/- Semua kalimat dijalankan secara bersamaan."

Terdakwa membayar sejumlah denda dan dia ditempatkan di Penjara Pusat, Chennai. Ini dianggap sebagai kasus pertama yang dihukum berdasarkan pasal 67 Undang-Undang Teknologi Informasi 2000 di India.

18.5 KASUS INDIA TERKAIT KEJAHATAN Cyber-II

Kasus Baazee.com: CEO Baazee.com ditangkap pada Desember 2004 karena CD dengan materi yang tidak pantas dijual di situs web. CD itu juga dijual di pasar-pasar di Delhi. Polisi kota Mumbai dan Polisi Delhi beraksi. CEO kemudian dibebaskan dengan jaminan. Ini membuka pertanyaan tentang perbedaan seperti apa yang kami buat antara Penyedia Layanan Internet dan Penyedia Konten. Beban terletak pada terdakwa bahwa dia adalah Penyedia Layanan dan bukan Penyedia Konten. Ini juga menimbulkan banyak masalah tentang bagaimana polisi harus menangani kasus kejahatan dunia maya dan banyak pendidikan diperlukan.

Penipuan Call Center Citibank MphasiS Pune: Rp 5.250.000.000 dari rekening empat nasabah AS secara tidak jujur ditransfer ke rekening palsu. Ini akan memberikan banyak amunisi kepada mereka yang melobi terhadap outsourcing di AS. Kasus-kasus seperti itu terjadi di seluruh dunia tetapi ketika itu terjadi di India, ini adalah masalah serius dan kita tidak bisa mengabaikannya. Ini adalah kasus rekayasa sumber. Beberapa karyawan mendapatkan kepercayaan dari pelanggan dan mendapatkan nomor PIN mereka untuk melakukan penipuan. Mereka mendapatkan ini dengan kedok membantu pelanggan keluar dari situasi sulit. Keamanan tertinggi berlaku di pusat panggilan di India karena mereka tahu bahwa mereka akan kehilangan bisnis mereka.

Tidak ada banyak pelanggaran keamanan tetapi rekayasa sumber. Karyawan call center diperiksa ketika mereka masuk dan keluar sehingga mereka tidak dapat menyalin nomor dan oleh karena itu mereka tidak dapat mencatatnya. Mereka pasti ingat nomor-nomor ini, langsung pergi ke warnet dan mengakses rekening Citibank nasabah. Semua akun dibuka di Pune dan pelanggan mengeluh bahwa uang dari akun mereka ditransfer ke akun pune dan begitulah cara para penjahat dilacak. Polisi telah berhasil membuktikan kejujuran call center tersebut dan telah membekukan rekening tempat uang tersebut ditransfer. Ada kebutuhan untuk pemeriksaan latar belakang yang ketat dari eksekutif pusat panggilan. Namun, pemeriksaan latar belakang terbaik tidak dapat menghilangkan elemen buruk yang masuk dan melanggar keamanan. Kami masih harus memastikan pemeriksaan tersebut ketika seseorang dipekerjakan. Ada kebutuhan untuk ID nasional dan basis data nasional di mana nama dapat dirujuk. Dalam kasus ini penyelidikan awal tidak mengungkapkan bahwa para penjahat memiliki sejarah kejahatan. Edukasi pelanggan sangat penting agar pelanggan tidak terbawa arus. Sebagian besar bank bersalah karena tidak melakukan ini.

18.6 KISAH KEJAHATAN DUNIA MAYA TERATAS-I:

1. Bisnis perlu menganggap serius kejahatan siber, kata polisi siber UE Trowels Orting

Bisnis perlu menangani kejahatan siber dengan sangat serius, menurut Trowels Orting, kepala Pusat Kejahatan Siber Eropa Europol. “Pada suatu waktu atau lainnya, semua bisnis kemungkinan akan terkena kejahatan dunia maya karena dunia menjadi semakin online,” kata Orthing kepada Computer Weekly. “Perusahaan yang tidak menganggap keamanan informasi penting harus mempertimbangkan kembali; jika tidak, mereka bisa berakhir berbisnis.” Ancaman kejahatan dunia maya jauh lebih besar daripada yang dipikirkan kebanyakan orang, katanya, karena sebagian besar masih tidak dilaporkan. “Kami tahu banyak kejahatan dunia maya yang sangat merugikan bisnis yang tidak dilaporkan ke polisi,” kata Orting percaya bisnis yang berinvestasi dalam proses, prosedur, dan teknologi yang tepat akan dihargai dalam jangka panjang – tetapi kegagalan untuk melakukannya jadi bisa berakibat fatal.

2. Model layanan yang mendorong kejahatan dunia maya, kata laporan Europol
   Industri pendukung kejahatan dunia maya menjadi semakin dikomersialkan, menurut sebuah laporan yang diterbitkan oleh Pusat Kejahatan Dunia Maya Eropa pada bulan September. Spesialis dalam ekonomi bawah tanah virtual sedang mengembangkan produk dan layanan untuk digunakan oleh penjahat dunia maya lainnya, kata laporan Penilaian Ancaman Kejahatan Terorganisir Internet (IOCTA). Penulis repot percaya model bisnis kejahatan sebagai layanan ini mendorong inovasi dan kecanggihan, dan menyediakan akses ke berbagai layanan yang memfasilitasi hampir semua jenis kejahatan dunia maya. Akibatnya, hambatan masuk untuk kejahatan dunia maya diturunkan untuk memungkinkan mereka yang tidak memiliki keahlian teknis – termasuk kelompok kejahatan terorganisir tradisional – untuk melakukan kejahatan dunia maya. Laporan tersebut juga menyoroti penyalahgunaan layanan dan alat yang sah seperti anonimisasi, enkripsi dan mata uang virtual, serta penyalahgunaan "kegelapan" untuk perdagangan gelap narkoba, senjata, barang curian, data pribadi dan kartu pembayaran yang dicuri, identitas palsu. dokumen dan materi pelecehan anak.
3. memimpin satuan tugas kejahatan dunia maya yang membuktikan nilainya, kata polisi dunia maya UE
   Hanya satu bulan dalam enam bulan percontohan, kejahatan dunia maya internasional yang dipimpin Inggris tampaknya akan menjadi permanen, Trowels Orting, kepala Pusat Kejahatan Dunia Maya Eropa (EC3) mengatakan pada bulan Oktober. EC3 menjadi tuan rumah Joint Cybercrime Action Taskforce (J-Cat) yang dibentuk pada September 2014 untuk mengoordinasikan investigasi internasional dengan mitra, menargetkan ancaman kejahatan dunia maya utama dan target utama. Diprakarsai oleh EC3, Satuan Tugas Kejahatan Dunia Maya UE, FBI, dan Badan Kejahatan Nasional (NCA), J-Cat terdiri dari petugas penghubung dunia maya dari negara-negara UE, mitra penegakan hukum non-Uni Eropa, dan EC3. Oerting mengatakan unit tersebut, yang dipimpin oleh wakil direktur Unit Kejahatan Siber Nasional (NCCU) UK‖m Andy Archibald, dijadwalkan untuk evaluasi pertama pada akhir Februari 2015. “Sudah ada indikasi akan diperpanjang setidaknya enam bulan lagi, tapi saya pikir kemungkinan akan permanen karena terus mendapatkan kasus dan kami berusaha mendapatkan Pendanaan Uni Eropa (UE) untuk itu,” katanya.

4. Operasi Inggris menjaring 17 tersangka penyerang cyber Blackshades
   Pada bulan Mei, operasi kejahatan dunia maya pertama di Inggris menjaring 17 tersangka pengguna malware Blackshades, yang dirancang untuk mengambil alih kendali komputer dan mencuri informasi. Dikoordinasikan oleh Badan Kejahatan Nasional yang baru, operasi selama seminggu di bulan Mei melibatkan hampir setiap unit kejahatan terorganisir regional Inggris serta Polisi Skotlandia dan Polisi Metropolitan. Investigasi Inggris adalah bagian dari aktivitas global yang menargetkan pengembang dan pengguna produktif Blackshades, seperangkat alat malware yang dijual online dengan harga kurang dari Rp 100.000. Dalam operasi yang diprakarsai oleh FBI dan dikoordinasikan di Eropa melalui Eurojust dan European Cybercrime Center di Europol, pasukan polisi secara internasional menangkap lusinan pengguna yang dicurigai. Penangkapan terjadi di Inggris, Belanda, Belgia, Finlandia, Austria, Estonia, Denmark, Kanada, Chili, Kroasia dan Italia, sehingga jumlah total penangkapan sehubungan dengan Blackshades menjadi 97. Produk Blackshades yang paling umum adalah akses jarak jauh tool (Rat), yang memungkinkan penjahat cyber untuk mengambil alih dan mengontrol operasi komputer yang terinfeksi dari jarak jauh.
5. Pasar gelap jatuh dalam operasi kejahatan anti-cyber internasional
   Penegak hukum internasional menurunkan beberapa pasar gelap yang beroperasi di jaringan Tor tersembunyi dan menangkap 17 tersangka kejahatan dunia maya pada awal November. Operation Ominous melibatkan petugas penegak hukum dari 16 negara bagian Eropa dan AS dalam salah satu operasi anti-cyber crime terbesar hingga saat ini. Operasi itu bertujuan untuk menghentikan penjualan, distribusi, dan promosi barang-barang ilegal dan berbahaya, termasuk senjata dan obat-obatan melalui pasar gelap online. Operation Onymous dikoordinasikan dari European Cybercrime Center Europol di Den Haag dan didukung oleh Joint Cybercrime Action Taskforce (J-Cat) yang dipimpin Inggris. Operation Onymous adalah kesuksesan besar kedua J-Cat hanya dalam waktu satu bulan dari enam bulan pilot, dan terjadi hanya beberapa minggu setelah Operation Imperium, yang mengakibatkan 31 penangkapan dan 42 pencarian rumah.

18.7 KISAH KEJAHATAN DUNIA MAYA TERATAS-II

6. Polisi Inggris melakukan empat penangkapan dalam penumpasan kejahatan dunia maya internasional
   Polisi Inggris melakukan empat penangkapan pada akhir November sebagai bagian dari tindakan keras internasional terhadap penjahat cyber yang menggunakan alat malware untuk membajak komputer dan mencuri data. Penggerebekan Inggris dipimpin oleh NCA, dan melibatkan petugas dari sejumlah Unit Kejahatan Terorganisir Regional (ROCU) polisi. Operasi internasional dikoordinasikan melalui Europol, dan difokuskan pada ancaman yang ditimbulkan oleh alat yang dikenal sebagai Trojan akses jarak jauh. Polisi di Estonia, Prancis, Rumania, Latvia, Italia, dan Norwegia melakukan 11 penangkapan lebih lanjut. Di Inggris, dua pria berusia 33 tahun dan seorang wanita berusia 30 tahun ditangkap di Leeds, dan seorang pria berusia 20 tahun ditangkap di Kent. Polisi mengeksekusi surat perintah penggeledahan pada seorang

pria berusia 19 tahun dari Liverpool, yang telah dibawa untuk diinterogasi secara sukarela. NCA mengatakan bahwa, selain menangkap orang yang diyakini menggunakan trojan akses jarak jauh, polisi menggunakan berbagai pendekatan untuk memperingatkan individu bahwa setiap gerakan ke dalam kejahatan dunia maya akan menghasilkan tindakan lebih lanjut.

7. Lebih dari seratus penjahat cyber ditangkap dalam operasi global
   Lembaga penegak hukum di seluruh dunia menangkap 118 tersangka, termasuk sekitar 40 di Inggris, dalam operasi kejahatan dunia maya internasional ketiga dari jenisnya pada akhir November. Operasi tersebut dipimpin oleh European Cybercrime Center Europol di Den Haag dan berkoordinasi dengan bantuan Interpol di Singapura dan Ameripol di Bogota. Operasi tersebut bertujuan untuk mengatasi penipuan online dan dilakukan bekerja sama dengan industri penerbangan, perjalanan dan kartu kredit. Lebih dari 60 maskapai penerbangan dan 45 negara terlibat dalam kegiatan yang berlangsung di lebih dari 80 bandara di seluruh dunia. Tindakan terkoordinasi tersebut menargetkan penjahat yang diduga melakukan penipuan membeli tiket pesawat secara online menggunakan data kartu kredit curian atau palsu. Dalam banyak kasus terungkap bagaimana penipuan kartu kredit memiliki kaitan atau memfasilitasi bentuk-bentuk kejahatan serius lainnya, seperti perdagangan narkoba.
8. Unit Kejahatan Siber Nasional Inggris terbuka untuk bisnis
   Unit Kejahatan Siber Nasional Inggris (NCCU) terbuka untuk bekerja dengan bisnis dan organisasi lain di sektor swasta, menurut wakil direktur Andy Archibald. “Bisnis dipersilakan untuk menghubungi kami dalam aksi kejahatan dunia maya yang bergerak langsung, dan kami akan bekerja dengan mereka untuk memastikan mereka mendapatkan tanggapan yang paling tepat,” katanya kepada Computer Weekly. NCCU melihat hubungan yang lebih dalam, lebih jelas dan berkembang dengan bisnis sektor swasta sebagai hal yang penting, tidak hanya untuk mengidentifikasi kejahatan dan pola kegiatan kriminal, tetapi juga untuk memanfaatkan keterampilan khusus. “Kita harus dapat pergi ke organisasi di sektor swasta dan meminta untuk bekerja dengan orang-orang dengan keterampilan yang kita butuhkan dalam beberapa penyelidikan”, kata Archibald. "Industri dapat membawa hal-hal ke meja yang mungkin tidak kita sadari, dan kami akan bekerja dengan sektor swasta dalam hukum jika solusi untuk operasi adalah sesuatu yang dapat dipimpin oleh sektor swasta."
9. Polisi Inggris menghadapi kurva pembelajaran yang curam tentang kejahatan dunia maya
   Polisi Inggris menghadapi kurva pembelajaran yang curam dalam mengatasi kejahatan dunia maya, tetapi beberapa inisiatif yang sedang berlangsung diarahkan untuk meningkatkan kemampuan dan kapasitas, Kelompok Kerja Kejahatan Online Polisi dan Komite Kejahatan dari Majelis London mendengar pada bulan November. Kelompok kerja sedang mengumpulkan bukti tentang tanggapan dari Layanan Polisi Metropolitan untuk kejahatan cyber-enabled. Ditanya apakah pemolisian berada di belakang kurva dalam hal mengatasi kejahatan yang dimungkinkan oleh dunia maya, CEO College of Policing Alex Marshall mengatakan jelas ada respons yang tidak konsisten terhadap ancaman ini. “Ada banyak hal yang harus dilakukan,” katanya dengan petugas yang

berpengalaman semakin harus berurusan dengan masalah kompleks, online dan dunia maya, yang pada awalnya tidak pernah dilatih untuk mereka. Marshall mengatakan College of Policing yang berusia 18 bulan berencana untuk menerbitkan standar nasional baru untuk penyelidikan dan intelijen online pada tahun 2015 untuk menggantikan standar usang yang diterbitkan pada tahun 2010. Perguruan tinggi tersebut juga telah mengembangkan sejumlah besar kursus pelatihan online untuk polisi di Inggris dan Wales. , serta kursus khusus untuk berbagai bidang keterampilan dalam kejahatan dunia maya atau online.

10. Penjahat dunia maya akan menjadi penyalur informasi, kata Web sense

    Penjahat dunia maya ditetapkan untuk menjadi penyalur informasi di tahun mendatang, menurut 10 prediksi keamanan cyber teratas untuk tahun 2015 oleh Web sense Security Labs. Analis keamanan utama Web sense Carl Leonard mengatakan penjahat akan menggunakan penjualan nomor kartu kredit untuk mendanai pengumpulan data yang lebih luas tentang korban. “Pasar bawah tanah dibanjiri dengan data kartu kredit curian, tetapi itu akan membantu mendanai pengumpulan kumpulan informasi pribadi yang lebih lengkap dan lebih kaya tentang individu,” katanya kepada mingguan komputer. Kumpulan data ini akan jauh lebih menguntungkan daripada perincian kartu kredit di pasar bawah tanah dan akan mencakup perincian beberapa kartu kredit, serta data regional, geografis, perilaku, dan pribadi. Web sense mengharapkan perdagangan yang muncul dalam kumpulan data pada individu ini akan memungkinkan pencurian identitas tingkat baru untuk memungkinkan penipuan.

18.8 HUKUM KASUS INDIA-I

Hukuman pertama di India: Pengaduan diajukan oleh Sony India Private Ltd yang menjalankan situs web bernama sony-sambandh.com, menargetkan Non Penduduk India. Situs web ini memungkinkan NRI mengirim produk Sony ke teman dan kerabat mereka di India setelah mereka membayarnya secara online.

Perusahaan menyanggupi untuk mengirimkan produk ke penerima yang bersangkutan. Pada bulan Mei 2002, seseorang masuk ke situs web dengan identitas Barbara Campa dan memesan satu set Sony Color Television dan telepon kepala nirkabel. Seorang wanita memberikan nomor kartu kreditnya untuk pembayaran dan meminta agar produk dikirim ke Arif Azim di Noida. Pembayaran telah diselesaikan oleh agen kartu kredit dan transaksi diproses. Setelah mengikuti prosedur due diligence dan pengecekan terkait, perusahaan menyerahkan barang tersebut kepada Arif Azim. Pada saat pengiriman, perusahaan mengambil foto digital yang menunjukkan pengiriman diterima oleh Arif Azim.

Transaksi ditutup pada saat itu, tetapi setelah satu setengah bulan agen mobil kredit memberi tahu perusahaan bahwa ini adalah transaksi yang tidak sah karena pemilik sebenarnya telah menyangkal telah melakukan pembelian. Perusahaan mengajukan keluhan atas kecurangan online di Biro Investigasi Pusat yang mendaftarkan kasus di bawah Bagian 418, 419 dan 420 KUHP India.

Masalah ini diselidiki dan Arif Azim ditangkap. Investigasi mengungkapkan bahwa Arif Azim, saat bekerja di call center di Noida memperoleh akses ke nomor kartu kredit warga

negara Amerika yang disalahgunakannya di situs perusahaan. CBI memulihkan televisi berwarna dan telepon kepala nirkabel. Terdakwa mengakui kesalahannya dan pengadilan Shri Gulshan Kumar Metropolitan Magistrate, New Delhi, menghukum Arif Azim berdasarkan Bagian 418, 419 dan 420 KUHP India - ini adalah pertama kalinya kejahatan dunia maya dihukum.

Namun, pengadilan merasa bahwa karena terdakwa adalah seorang anak laki-laki berusia 24 tahun dan baru pertama kali menjadi narapidana, pandangan yang lunak perlu diambil. Oleh karena itu, pengadilan membebaskan terdakwa dengan masa percobaan selama satu tahun.

18.9 HUKUM KASUS INDIA-II

Kasus terkait postingan pesan cabul, fitnah, dan menjengkelkan tentang wanita cerai di grup pesan yahoo. E-mail juga diteruskan kepada korban untuk informasi oleh terdakwa melalui akun e-mail palsu yang dibukanya atas nama korban. Postingan pesan tersebut mengakibatkan panggilan telepon yang mengganggu ke wanita itu dengan keyakinan bahwa dia meminta.

Berdasarkan pengaduan yang dibuat oleh korban pada Februari 2004, Polisi melacak tersangka ke Mumbai dan menangkapnya dalam beberapa hari ke depan. Terdakwa adalah teman keluarga korban yang dikenal dan dilaporkan tertarik untuk menikahinya. Namun dia menikah dengan orang lain. Pernikahan ini kemudian berakhir dengan perceraian dan terdakwa mulai menghubunginya sekali lagi. Karena keengganannya untuk menikah dengannya, terdakwa melakukan pelecehan melalui Internet.

Pada 24-3-2004 Charge Sheet diajukan u/s 67 dari IT Act 2000, 469 dan 509 IPC Sebelum Yang Mulia Addl. CMM dengan mengutip 18 saksi dan 34 dokumen dan objek material. Hal yang sama diambil pada file di C.C.NO.4680/2004. Di sisi penuntutan 12 saksi diperiksa dan seluruh dokumen ditandai. Pembela berpendapat bahwa surat-surat yang menyinggung akan diberikan baik oleh mantan suami pelapor atau pelapor sendiri untuk melibatkan terdakwa karena dituduh telah menolak permintaan pelapor untuk menikahinya. Lebih lanjut, Penasihat Hukum berargumen bahwa beberapa bukti dokumenter tidak dapat dipertahankan berdasarkan Bagian 65 B dari Undang-Undang Bukti India. Namun, pengadilan berdasarkan saksi ahli Naavi, bukti lain yang dihasilkan termasuk saksi pemilik Warnet sampai pada kesimpulan bahwa kejahatan itu terbukti secara meyakinkan.

Pengadilan juga menyatakan bahwa karena investigasi teliti yang dilakukan oleh IO, asal mula pesan cabul itu dapat dilacak dan pelaku sebenarnya telah dibawa ke pengadilan. Dalam hal ini Sri S. Kothandaraman, Jaksa Penuntut Umum Khusus yang ditunjuk oleh Pemerintah melakukan kasus tersebut. Yang Mulia Sri.Arulraj, Additional Chief Metropolitan Magistrate, Egmore, menyampaikan putusan pada 11-05-04 sebagai berikut:

“Terdakwa dinyatakan bersalah melakukan pelanggaran berdasarkan pasal 469, 509 IPC dan 67 IT Act 2000 dan terdakwa dinyatakan bersalah dan dihukum karena pelanggaran tersebut untuk menjalani RI selama 2 tahun di bawah 469 IPC dan membayar denda Rs.500 /- dan untuk pelanggaran u/s 509 IPC divonis 1 tahun penjara Sederhana dan membayar denda Rs.500/- dan untuk pelanggaran u/s 67 UU IT 2000 menjalani RI selama 2 tahun dan membayar denda Rs. .4000/- Semua Kalimat untuk dijalankan secara bersamaan.

18.10 HUKUM KASUS INDIA-III

Pengadilan Distrik dan Sidang Tambahan di sini telah menguatkan putusan pengadilan yang lebih rendah dalam kasus dunia maya pertama yang diajukan di Negara Bagian yang menghukum seorang imam Gereja Pantekosta dan putranya dengan hukuman penjara yang ketat pada tahun 2006. Membuang banding yang diajukan oleh pendeta T.S. Balan dan putranya, Aneesh Balan, melawan perintah Hakim Ketua, pada hari Rabu, Hakim Distrik Tambahan T.U. Mathewkutty mengatakan sudah saatnya pemerintah mengambil langkah-langkah efektif untuk memeriksa tren kejahatan dunia maya yang berkembang di negara bagian tersebut.

Pengadilan menguatkan perintah hakim yang menghukum dua sampai tiga tahun ketat penjara dan denda sebesar Rp. 25.000 berdasarkan Pasal 67 dari Undang-Undang teknologi informasi (TI); memberikan hukuman enam bulan penjara berdasarkan Bagian 120(B) KUHP India; dan memerintahkan satu tahun penjara yang ketat dan menjatuhkan denda Rs. 10.000 di bawah Bagian 469 dari kode. Pengadilan mencabut hukuman berdasarkan Pasal 66 UU IT. Kasus siber terjadi pada Januari-Februari 2002 dan imam serta putranya menjadi orang pertama yang dihukum karena melakukan kejahatan siber. Keduanya dinyatakan bersalah atas morphing, web-hosting dan e-mail gambar telanjang Pastor Abraham dan keluarganya.

Balan telah bekerja dengan pendeta sampai dia berselisih dengannya dan ditunjukkan pintu oleh pendeta itu. Balan bergabung dengan Gereja Pantekosta Sharo. Penuntut mengatakan keduanya telah mengubah foto-foto Abraham, putranya, Valsan Abraham, dan putrinya, Starla Luke, dan mengirim email kepada mereka dari ID surat palsu dengan keterangan. Gambar-gambar yang diubah itu ditempatkan di web dan terdakwa, yang mengedit sebuah majalah lokal bernama The Defender, menulis tentang foto-foto ini dalam publikasinya. Valsan menerima foto-foto itu di Internet dan meminta ayahnya untuk mengajukan pengaduan ke polisi. Sebuah kelompok polisi menggerebek rumah Balan dan putranya di Perumbavoor dan mengumpulkan barang bukti.

Putusan hakim datang setelah persidangan empat tahun, di mana pengadilan harus membeli komputer dengan koneksi internet dan aksesori. Polisi juga harus mengamankan jasa seorang analis komputer untuk mengumpulkan bukti-bukti. Dua puluh sembilan saksi, termasuk penyedia layanan Internet dan Bharat Sanchar Nigam Ltd., harus diberhentikan di depan pengadilan.100

18.11 RINGKASAN

Isu kejahatan dunia maya dapat dipahami melalui studi kasus dengan mudah daripada lebih fokus pada aspek teoritis. Isu-isu yang terkait dengan kejahatan dunia maya dibahas melalui studi kasus kejahatan dunia maya di Inggris, kasus-kasus Asia-Pasifik yang dipilih, kasus-kasus India yang terkait dengan kejahatan dunia maya dan kisah-kisah kejahatan dunia maya teratas dan hukum kasus India dibahas untuk pemahaman yang lebih baik melalui ilustrasi dan contoh yang tepat.

18.12 BEBERAPA BUKU BERGUNA

- Black Ice: Ancaman Tak Terlihat dari Terorisme Cyber oleh Dan Verton (Publikasi Profesional Mc Graw Hill)

- Kejahatan Siber dan Terorisme Siber oleh R.K. Pradhan (Publikasi Mangalam)
- Kejahatan Siber dan Terorisme Siber oleh Vinod Kumar Jayaswal (Penerbit dan Distributor Neha)
- Terorisme Cyber oleh S. Venkatesh (Authorpress)
- Keamanan Kripto dan Jaringan oleh Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Undang-Undang Teknologi Informasi, 2000: Pergeseran Paradigma Konseptual dalam Hukum oleh Divya Chansoria dan Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Kejahatan Cyber dan Teknologi Informasi oleh Vikram Singh Jaswal (Publikasi Regal)
- Panduan Hukum Cyber (Undang-Undang Teknologi Informasi, 2000. E-Commerce, Perlindungan Data dan Internet) oleh Rodney D Ryder (Lexis Nexis-India)
- Buku Pegangan Keamanan, Kriptografi, dan Tanda Tangan Digital oleh P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Hukum Cyber dan Perlindungan TI oleh Harsh Cander (Publikasi PHI)
- Pengantar Hukum Cyber oleh Dr. J.P. Mishra (Publikasi Hukum Pusat)
- Perang Cyber dan Terorisme oleh Mithilesh K. Singh (Rumah Penerbitan Prashant)
- Terorisme Cyber: Implikasi Politik dan Ekonomi oleh Andrew M. Colarik (Penerbitan Grup Ide)
- Terorisme dan Hukum Cyber oleh S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- Kekeliruan Netralitas Bersih oleh Thomas W. Hazlett (Encounters Books)
- Akses ke Jaringan Broadband: Debat Netralitas Net (Buat Ruang Publikasi)
- Ruang Siber dan Keamanan Siber oleh Manajemen Progresif (Publikasi Manajemen Progresif)
- Komputer, Privasi, dan Perlindungan Data: Elemen Pilihan (Springer)
- Semua Situs Web yang Relevan dikutip di tempat yang tepat dalam materi studi untuk referensi siap pakai. Penulis tidak mengklaim hak apa pun sehubungan dengan materi yang dikutip itu.

18.13 PERIKSA KEMAJUAN ANDA

A. Manakah dari pernyataan berikut ini yang benar atau salah:

a. Menghentikan kejahatan dunia maya dapat berdampak positif terhadap ekonomi dunia.
b. Biaya paling penting dari kejahatan dunia maya berasal dari kerusakannya terhadap kinerja perusahaan dan ekonomi nasional.
c. Teknologi seperti ponsel dan jejaring sosial semakin terancam oleh penjahat cyber.
d. Industri AS memperkirakan nilai barang palsu di China sebesar Rp 285.000 miliar hingga Rp 360.000 miliar.
e. Lembaga penegak hukum di seluruh dunia menangkap 118 tersangka, termasuk sekitar 40 di Inggris, dalam operasi kejahatan dunia maya internasional ketiga dari jenisnya.

B. Isi Bagian yang Kosong:

I. Dalam ……., pemerintah Inggris mendokumentasikan dalam laporan resmi bahwa biaya keseluruhan ekonomi kejahatan dunia maya adalah…….
II. Reporte, china telah menjadi …… barang palsu dan bajakan di dunia.
III. ……ditangkap pada bulan Desember 2004 karena CD dengan materi yang tidak pantas dijual di situs web.
IV. Industri pendukung kejahatan dunia maya menjadi semakin ……..
V. ……., misalnya, kerugian peretasan yang sebenarnya berjumlah $ 875 juta tetapi pemulihan, atau biaya pembersihan mencapai $ 8,5 miliar.

18.14 JAWABAN UNTUK MEMERIKSA KEMAJUAN ANDA

A.

1. Benar
2. Benar
3. Benar
4. Benar
5. Benar

B.

1. 2011; Rp 405.000 miliar setahun
2. Eksportir Terkemuka
3. CEO Bazze.com
4. Dikomersialkan
5. Di Italia

18.15 PERTANYAAN TERMINAL

1. Membahas secara rinci kejahatan dunia maya di Inggris.
2. Diskusikan kasus-kasus Asia-Pasifik yang dipilih.
3. Membahas kasus-kasus India terkait kejahatan dunia maya-I.
4. Membahas kasus-kasus India terkait cyber crime-II.
5. Diskusikan cerita kejahatan dunia maya teratas.

DAFTAR PUSTAKA

A. Infantono, J. Budiarto, A. Persada, F. Azzuhri, and Z. Abidin, “Content Filtering Pornografi Halaman Web Berbasis Citra dan Teks pada Sistem Terintegrasi Server Internet”, AAU-JDST, vol. 5, no. 2, pp. 125-132, Jan.2021

Anne W. Brascomb (ed), Toward A Law of Global Communication Network, New York: Lognman, 1986.

Ardiyanti, Handrini. 2014. “Cyber-Security dan Tantangan Pengembangannya di Indonesia”. Jurnal Politica. Vol. 5. No. 1 . Juni.

Arianto, Adi Rio. 2017. “Cyber Security: Geometripolitika dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21”. Jurnal Power In International Relations. Universitas Potensi Utama. Vol. 1. No.2. Februari.

B.L. Berg, H. Lune, Qualitative Research methods for The Social Sciences, ninth edition, (England, Essex: Pearson Education Limited, 2017).

Badri, Muhammad. 2011. Perang cyber dalam dinamika komunikasi internasional dalam buku Komunikasi militer, Aspikom.

Barrinha A, Renard T. “Cyber-diplomacy: the making of an International society in the digital age”. Global Affairs, (2017)

Brascomb, Anne W. 1986. Toward A Law of Global Communication Network. USA: Longman.

Buzan, Barry. 1998. Security: A Framework for Analysis. Boulder: Lynne Reinner Publishers.

C. Bilah and A. Infantono, “Pengembangan Aplikasi Mobile Kamus Istilah Aeronautika pada Platform Android Sesuai Standar ISO 25010”, senastindo, vol. 1, pp. 195-202, Oct. 2021.

Chintia, E. dkk. 2019. Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. Journal of Information Engineering and Educational Technology.

Ghernaouti, Solange. 2013. Cyber Power: Crime, Conflict and Security in Cyberspace. Lausanne: EPFL Press.

Igwe, K., & Ibegwam, A. 2014. Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria. International Journal of ICT and Management II.

Indrawan, Raden Mas Jerry dan Efriza. 2017. “Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia”. Jurnal Pertahanan dan Bela Negara. Universitas Pertahanan Indonesia. Vol. 7.No. 3. Desember.

John Vivian. 2008. Teori Komunikasi Massa, Jakarta: Kencana.

Koh, B. (t.t.): Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do about It, HarperCollins Publishers, 2010.

M. Arsyad Sanusi. 2005. Hukum Teknologi dan Informasi, Bandung: Tim Kemas Buku, 2005

Menthe, D. 1998. “Jurisdiction in Cyberspace: A Theory of International Space”. Michigan Telecommunications and Technology Law.

Pusat Operasi Keamanan Siber Nasional, Laporan Tahun 2020 (Monitoring Keamanan Siber). Jakarta: Badan Siber Dan Sandi Negara, 2020.

Pusat Teknologi Informasi dan Komunikasi Badan Pengkajian dan Penerapan Teknologi (BPPT), Kajian Konvergensi Teknologi Informasi dan Komunikasi, Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT, 2007

Ronald Thompson & William Cats Barril, Information Technology and Management, New York: Mc Graw Hill, 2003.

Sanjaya, M. B. 2017. Inisialisasi Key Generating Kriptografi AES Pada Pendekatan Protokol SMSSEC. Jurnal Infotel, 9(1), 18-23.

Sanjaya, M. B. 2017. Inisialisasi Key Generating Kriptografi AES Pada Pendekatan Protokol SMSSEC. Jurnal Infotel.

Sanusi, M. Arsyad. 2005. Hukum Teknologi dan Informasi. Bandung: Tim Kemas Buku.

Sitompul, Josua. 2012. Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana. Jakarta: PT. Tatanusa.

Sultana, S., Jabiullah, M. I., & Rahman, M. L. 2009. Improved Needham-Schroeder protocol for secured and efficient key distributions. 2009 12th International Conference on Computers and Information Technology.

Sultana, S., Jabiullah, M. I., & Rahman, M. L. 2009. Improved Needham-Schroeder protocol for secured and efficient key distributions. 2009 12th International Conference on Computers and Information Technology.

Syah, R. D., & Suhatril, R. J. 2019. Digital Image Cryptography Using Combination of Arnold's Cat Map and Bernoulli Map Based on Chaos Theory.

Syah, R. D., & Suhatril, R. J. 2019. Digital Image Cryptography Using Combination of Arnold's Cat Map and Bernoulli Map Based on Chaos Theory,

Thompson, Ronald & William Cats Barril. 2003. Information Technology and Management. New York: Mc Graw Hill.

Vivian, John. 2008.Teori Komunikasi Massa. Jakarta: Kencana.

Winarno., Budi. Dinamika Isu-isu Global Kontemporer. (Yogyakarta: CAPS. 2014)

KEAMANAN SIBER

(CYBER SECURITY)

Fujiama Diapoldo Silalahi S.Kom, M.Kom

BIO DATA PENULIS

Penulis buku ini adalah dosen Universitas Sains dan Komputer bernama Fujiama Diapoldo Silalahi, S.Kom, M.Kom. Lahir pada tanggal 10 Nopember 1982 dan penulis saat ini menjabat sebagai Wakil Rektor 3 Bidang Perencanaan, Keuangan dan Sistem Informasi penulis memiliki Riwayat pendidikan S1 Sekolah Tinggi Elektronika dan Komputer, S2 Universitas Dian Nuswantoro Semarang.

Saat ini penulis adalah Dosen tetap di Universitas Sains dan Teknologi Komputer (Universitas STEKOM) pada program studi S1 Teknik Informatika serta memiliki Jabatan Fungsional Lektor dan mengampu mata kuliah antara lain Keamanan Jaringan, Cyber Security, Pemrograman Visual, Pemrograman Web Server, Database Server, Teknologi Informasi.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :

YAYASAN PRIMA AGUS TEKNIK

JL. Majapahit No. 605 Semarang

Telp. (024) 6723456. Fax. 024-6710144

Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-5734-81-1 (PDF)

9 786235 734811

Fujiama Diapoldo Silalahi S.Kom, M.Kom

KEAMANAN SIBER

(CYBER SECURITY)

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
JL. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id