kejahatan di dunia maya atau sering disebut dengan istilah kejahatan siber (*cybercrime*) merupakan sebuah aktivitas kejahatan yang dilakukan di dunia maya dengan memanfaatkan perangkat komputer melalui media komunikasi (jaringan) lokal, privat, dan/atau public (Internet) sebagai alat untuk melakukan kejahatan. Jadi, *cybercrime* memiliki dua pengertian yaitu secara arti luas merupakan segala tindakan ilegal (tidak sah) yang dilakukan dengan menggunakan jaringan komputer lokal (privat) dan Internet (publik) sehingga si pelaku mendapatkan keuntungan sepihak dengan merugikan pihak lain. Pengertian lainnya yang lebih sempit dari *cybercrime* adalah segala bentuk tindakan ilegal yang bertujuan untuk menguji, menyerang, dan/atau melumpuhkan sistem keamanan dan data yang diproses oleh sebuah sistem komputer.

Kejahatan siber (*cybercrime*) terjadi karena beberapa sebab di antaranya adalah:

1. Aksi coba-coba dikarenakan si pelaku sedang belajar cara meretas sistem dan mempraktikkan apa yang dibacanya dari suatu artikel atau buku;
2. Aksi ingin tenar atau mencari nama dengan meretas sebuah sistem;
3. Aksi sebagai tindakan bersenang-senang;
4. Aksi sebagai hobi untuk mencari kelemahan sistem;
5. Akses sebagai perusak sistem seperti *hacker* dan *cracker* yang memang sengaja meretas sistem untuk merusak data, aplikasi, dan layanannya.

Perang siber tampaknya mendominasi berita utama akhir-akhir ini. Baik itu kelompok yang meretas komputer untuk 'bersenang-senang' atau dugaan lembaga pemerintah yang mencoba mencuri informasi rahasia. Lanskap Internet telah berubah menjadi medan perang digital. Jika sudah demikian, siapa yang membutuhkan pistol ketika Anda memiliki sebuah *keyboard*?

Pada umumnya, kejahatan di dunia maya dilakukan melalui berbagai cara dan memiliki banyak tujuan. Tindakan kriminal ini telah terjadi sejak awal tahun 1980-an di mana pada saat itu terdapat insiden peretasan sebuah sistem komputer yang kemudian dikenal dengan istilah *Cyber Attack*. Pada masa itu, pelaku kejahatan siber menciptakan sebuah virus yang dikenal dengan istilah worm. Virus berupa worm ini diciptakan oleh Morris, seorang mahasiswa di Cornell Univeristy di AS, untuk menyerang jaringan komputer yang menyebabkan sekitar 6.000 komputer di seluruh dunia yang memiliki jaringan dan terkoneksi ke Internet mengalami mati total. Serangan ini merugikan sekitar 10-100 juta dolar Amerika untuk melakukan pemulihan sistemnya (ARN, 2021).

A. PENGERTIAN *CYBERCRIME* MENURUT PARA AHLI

Berikut merupakan beberapa pengertian kejahatan siber atau kejahatan di dunia maya (*cybercrime*) yang dikemukakan oleh para ahli, di antaranya:

1. Goutam (2021)

Cybercrime mengacu pada tindakan melawan hukum yang dilakukan dengan menggunakan komputer dan Internet dalam lingkungan digital yang saling terhubung. Mereka menggunakan dunia maya untuk tindakan ilegal dan mengeksploitasi fitur-fitur uniknya seperti kecepatan (*speed*), kedekatan (*immediacy*), dan enkripsi (*encryption*) untuk menyembunyikan aktivitas ilegal dan juga penjahat.

2. Shoemaker, Kohnke, dan Sigler (2020)

Istilah kejahatan siber/dunia maya (*cybercrime*) sering digunakan untuk mengidentifikasi tiga kategori aktivitas kriminal yang berbeda: kejahatan di mana infrastruktur siber hanyalah alat dari beberapa kejahatan tradisional lainnya (misalnya, penipuan keuangan), distribusi konten kriminal (misalnya, pornografi dan ujaran kebencian), dan kejahatan yang ditujukan terhadap infrastruktur siber

itu sendiri (misalnya, penyusupan yang melanggar hukum ke dalam sistem komputer) (Walden, 2016; Holt, Bossler, dan Seigfried-Spellar, 2018; Clough, 2015).

3. Widodo (2011) dan Suhariyanto (2014)

Cybercrime adalah semua kegiatan individu atau kelompok yang memakai jaringan komputer sebagai sarana melakukan kejahatan, atau menjadikan komputer sebagai sasaran kejahatan.

4. Wahid dan Labib (2009)

Cybercrime adalah semua jenis pemakaian jaringan komputer untuk tujuan kriminal dengan penyalahgunaan kemudahan teknologi digital.

5. Parker (1998)

Cybercrime merupakan sebuah tindakan atau kejadian yang melawan hukum (ilegal) berkaitan dengan teknologi komputer. Tindakan yang dilakukan memberikan keuntungan baginya dan merugikan pihak lainnya.

6. *Organization of European Community Development* (OECD)

Cybercrime adalah semua akses ilegal terhadap suatu transmisi data. Hal ini dapat diartikan bahwa semua kegiatan yang tidak sah dalam suatu sistem komputer termasuk suatu tindak kejahatan (Karnasudiraja, 1993).

B. KARAKTERISTIK *CYBERCRIME*

Kejahatan siber mencakup berbagai pelanggaran termasuk kejahatan terhadap data dan sistem, pemalsuan dan penipuan yang diaktifkan Internet, penyebaran konten seksual dan bajakan. Kejahatan siber masih belum memiliki definisi yang diterima secara global. Pengacara Amerika tidak dapat membenarkan kejahatan siber dengan kerangka hukum khusus yang digunakan di Amerika Serikat (Susan W. Brenner, 2007). Menurut Fafinski, Dutton, dan Margetts (2010), *cybercrime* memiliki teori tripartit yaitu:

1. kejahatan terhadap komputer,
2. kejahatan dalam komputer;
3. kejahatan melalui komputer.

Dalam kejahatan konvensional dikenal dua jenis kejahatan sebagai berikut:

1. Kejahatan Kerah Biru (*Blue Collar Crime*)

Kejahatan jenis ini merupakan tindak kriminal yang dilakukan secara konvensional yaitu kejahatan yang dilakukan secara langsung bertemu dengan korban atau berada di lokasi kejahatan. Contoh jenis kejahatan ini adalah perampokan, pencurian, pembunuhan, dan lainnya. Para pelaku kejahatan jenis ini biasanya digambarkan memiliki stereotip tertentu, misalnya, dari kelas sosial bawah, kurang terdidik, berpenghasilan rendah, dan lain sebagainya.

2. Kejahatan Kerah Putih (*White Collar Crime*)

Kejahatan jenis ini terbagi ke dalam empat kelompok kejahatan, yakni (1) kejahatan korporasi, (2) kejahatan birokrat, (3) malpraktek, dan (4) kejahatan individu. Pelakunya biasanya berkebalikan

dari *blue collar*, mereka memiliki penghasilan tinggi, berpendidikan, memegang jabatan-jabatan terhormat di masyarakat.

Cybercrime sendiri merupakan kejahatan yang terjadi dengan akibat adanya sebuah komunikasi siber melalui Internet, kejahatan siber memiliki karakteristik yang berbeda dengan kedua jenis kejahatan di atas. Karakteristik unik dari kejahatan di dunia maya tersebut antara lain menyangkut lima hal sebagai berikut.

a. Ruang lingkup kejahatan

Sesuai sifat global Internet, ruang lingkup kejahatan ini juga bersifat global. Pada umumnya *cybercrime* dilakukan dengan cara transnasional, di mana kejahatan tersebut melintasi batas negara yang sulit ditentukan yuridikasi hukum negara yang berlaku terhadap pelaku. Hal ini disebabkan karena karakteristik jaringan Internet yang berlalu-lalang tanpa identitas (*anonymous*) penggunanya. Hal tersebut memungkinkan adanya berbagai aktivitas kejahatan yang tidak tersentuh hukum.

b. Sifat kejahatan

Kejahatan di dunia maya (*cybercrime*) bersifat *non-violence* (tanpa kekerasan) dan tidak menimbulkan kekacauan yang mudah terlihat. Jika kejahatan konvensional sering kali menimbulkan kekacauan maka kejahatan di Internet bersifat sebaliknya.

c. Pelaku kejahatan

Pelaku kejahatan bersifat lebih universal, meski memiliki ciri khusus yaitu kejahatan dilakukan oleh orang-orang yang menguasai penggunaan Internet beserta aplikasinya. Pelaku kejahatan tersebut tidak terbatas pada usia dan stereotip tertentu, mereka yang sempat tertangkap adalah remaja, bahkan beberapa di antaranya masih anak-anak.

d. Modus kejahatan

Keunikan kejahatan ini adalah penggunaan teknologi informasi dalam modus operandi, itulah sebabnya mengapa modus operandi dalam dunia siber tersebut sulit dimengerti oleh orang-orang yang tidak menguasai pengetahuan tentang komputer, teknik pemrograman dan seluk beluk dunia siber.

e. Jenis kerugian yang ditimbulkan

Jenis kerugian dapat bersifat material maupun non-material. Seperti waktu, nilai, jasa, uang, barang, harga diri, martabat bahkan kerahasiaan informasi.

C. JENIS *CYBERCRIME*

Cybercrime merupakan bentuk kejahatan yang dilakukan di dunia maya. Berikut ini yang digolongkan berbagai jenis *cybercrime* yang dilihat dari sudut pandang yang berbeda. Pengelompokan jenis kejahatan siber ini berdasarkan pada jenis aktivitas, motif kegiatan, dan sasaran kejahatan, yaitu:

1. Berdasarkan Jenis Aktivitasnya

Berikut merupakan beberapa *cybercrime* yang dilakukan berdasarkan jenis aktivitasnya, di antaranya adalah:

a. Akses ilegal (unauthorized access)

Kejahatan ini merupakan jenis kejahatan yang disebabkan karena terjadinya suatu tindakan di mana seorang tindak kejahatan menyusup ke dalam sebuah sistem baik langsung atau melalui jaringan

komputer dengan cara tidak sah atau tanpa seizin pemilik sistem jaringan komputer yang dimasukinya. Berikut ini adalah beberapa contoh aktivitas ini:

1) *Probing* dan *Port Scanning* merupakan contoh dari kejahatan ini. Aktivitas *port scanning* atau *probing* dilakukan dengan tujuan untuk melihat jenis layanan (*services*) yang tersedia pada server target. Aktivitas hasil scanning dapat menunjukkan informasi bahwa server target menjalankan program *web server Apache*, *mail server Sendmail*, dan seterusnya.

   Ini dapat dianalogikan dalam dunia nyata seperti halnya seseorang mendatangi sebuah rumah lalu mengecek jumlah pintu dan jendela, tipe kuncinya, apakah pintu dan jendelanya terkunci atau tidak, merek kunci yang digunakannya, dan memiliki pagar atau tidak (ini gambaran jika menggunakan firewall, intrusion detection system/IDS), dan seterusnya.

   Program yang dapat digunakan dalam melakukan *probing* atau *portscanning* dapat diperoleh secara gratis pada jaringan Internet. Salah satu program yang paling populer adalah "*nmap*" (untuk sistem yang berbasis Unix dan Linux) dan "*Superscan*" (untuk sistem yang berbasis Micrososft Windows).

   Selain bertujuan untuk mengidentifikasikan *port*, *nmap* juga dapat digunakan untuk mengidentifikasi jenis operating system yang digunakan.

2) *Cyber-Tresspass* adalah pelanggaran area privasi pihak lain, baik individu atau organisasi seperti misalnya membobol akun PC atau mengirimkan Email Spam. Email spam adalah sebuah pelanggaran privasi dengan mengirimkan email yang tidak berguna atau email sampah yang ditujukan kepada seseorang.

b. Konten ilegal (illegal content)

Konten ilegal merupakan sebuah kejahatan siber yang dilakukan dengan cara memasukkan informasi atau data ke dalam jaringan Internet mengenai hal yang tidak benar, dan tidak etis sehingga dapat dianggap sebagai tindakan melanggar hukum atau mengganggu ketertiban umum. Kejahatan *illegal content* yang sering terjadi adalah tindakan penyebarluasan pornografi di dunia maya yaitu dengan membuat, memasang, mendistribusikan serta menyebarkan segala konten yang bersifat pornografi kemudian mengekspos hal-hal tersebut secara langsung di dunia maya. Selain konten yang bersifat pornografi, penyampaian berita bohong atau yang dikenal dengan istilah berita *hoaks* atau kabar burung merupakan contoh lain kejahatan jenis ini.

c. Penyebaran virus secara sengaja

Jenis kejahatan seperti ini sama halnya dengan kejahatan lainnya yang terjadi di dunia nyata, yaitu menyebarkan virus yang dapat merugikan orang lain. Menyebarkan virus pada jaringan komputer juga terjadi di Indonesia pada khususnya dan seluruh dunia pada umumnya. Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Hal yang terjadi adalah orang-orang tidak menyadari jika sistem emailnya terkena virus, selanjutnya menyebarkan virus tersebut melalui emailnya.

d. Data forgery

Data forgery merupakan jenis kejahatan yang dilakukan dengan tujuan untuk memalsukan data-data pada setiap dokumen yang ada di Internet. Dokumen-dokumen tersebut biasanya merupakan dokumen berbasis data web yang dimiliki oleh institusi atau lembaga. Dokumen tersebut kemudian disimpan sebagai dokumen *scriptless* dengan menggunakan media Internet. Salah satu praktik pemalsuan data ini misalnya pemalsuan dokumen pada kasus situs bank BCA pada tahun 2000-an dengan cara membuat situs serupa bank BCA dikarenakan akibat dari pemanfaatan ketidaktelitian dan kelengahan nasabahnya yang banyak melakukan *typo* (salah ketik) ketika mengunjungi alamat web

bank BCA. Akibatnya, si pelaku akan dapat dengan mudah merekam akun dan password nasabah. Contoh lain adalah dengan pemalsuan dokumen pada situs e-commerce yang dibuat seolah-olah terjadi salah ketik, sehingga menguntungkan pelakunya.

e. Cyber espionage, sabotage dan extortion

Cyber espionage merupakan jenis kejahatan dengan memanfaatkan jaringan Internet dalam melaksanakan semua kegiatan mata-mata yang dilakukan terhadap pihak lain. Kejahatan ini dilakukan dengan cara memasuki sebuah sistem jaringan komputer korban atau pihak sasaran. Langkah selanjutnya adalah melakukan *sabotage* dan *extortion* yaitu sebuah jenis kejahatan dengan melakukan tindakan berupa membuat gangguan, penghancuran terhadap suatu data, perusakan sistem program komputer, ataupun sebuah sistem jaringan komputer yang terhubung dengan Internet.

f. Cyber stalking

Jenis kejahatan ini dilakukan dengan tujuan mengganggu atau melecehkan seseorang dengan memanfaatkan media komputer. Salah satu contohnya adalah dengan menggunakan email yang dilakukan secara berulang-ulang. Bisa dikatakan bahwa jenis kejahatan ini merupakan kejahatan yang menyerupai teror. Kejahatan tersebut ditujukan untuk seseorang dengan memanfaatkan media Internet. Salah satu alasannya adalah mudahnya membuat alamat email baru yang digunakan pelaku untuk melakukan aksinya tanpa harus menyertakan identitasnya.

g. Pencurian data (data theft)

Pencurian data merupakan aktivitas mencuri data dari sistem komputer secara ilegal, baik untuk kepentingan sendiri atau dijual kepada pihak lain. Tindakan pencurian data ini sering berujung pada kejahatan penipuan (*fraud*) secara online.

h. Penyalahgunaan Kartu Kredit (Carding)

Carding adalah jenis kejahatan siber yang dilakukan dengan tujuan untuk mencuri nomor kartu kredit orang untuk digunakan dalam sebuah kegiatan transaksi perdagangan dalam jaringan Internet. Munculnya jenis kejahatan ini disebabkan karena adanya perkembangan pesat perdagangan yang memanfaatkan jaringan Internet yang dikenal dengan istilah (*e-commerce*) di mana transaksinya dilakukan secara elektronik.

i. Hacking and cracking

Hacker merupakan seseorang dengan minat sangat besar dalam mempelajari sistem komputer secara rinci dalam rangka meningkatkan kemampuan di bidang komputer. Mereka juga ingin mengetahui lebih dalam cara untuk meningkatkan kapabilitas sebuah komputer. Kejahatan jenis ini biasanya dilakukan karena adanya minat yang cukup tinggi yang dimiliki oleh seorang *hacker* untuk mengetahui sistem komputer dan sistem jaringan komputer lebih mendalam. Sesungguhnya *hacker* memiliki kencenderungan netral dan tidak merusak, sedangkan mereka yang biasanya melakukan aksi perusakan pada sistem komputer dan jaringan Internet lazim disebut sebagai *cracker* atau pembobol jaringan Internet.

Cracker dapat dikatakan seorang *hacker* yang memanfaatkan pengetahuan dan kemampuannya untuk melakukan hal-hal yang bersifat negatif di dunia maya. Aktivitas *cracking* pada jaringan Internet memiliki ruang lingkup sangat luas. Hal ini diawali dengan pembajakan akun milik orang lain, *probing*, pembajakan situs web, menyebarkan virus, hingga pelumpuhan target sasaran. Selanjutnya, kegiatan kejahatan terakhir yang dilakukan dikenal dengan istilah *DoS (Denial of Service).* Serangan *DoS* adalah

sebuah serangan dengan tujuan melumpuhkan target layanan agar target tidak dapat melakukan dan memberikan layanan apa pun sehingga orang lain tidak dapat mengakses layanan tersebut (*hang*, *crash*). Serangan jenis ini tidak bertujuan untuk melakukan pencurian, melakukan penyadapan maupun pemalsuan data. Akan tetapi, dengan hilangnya layanan maka target tidak dapat memberikan pelayanan sehingga ada kerugian finansial dan non-materi yang diakibatkannya. Salah satu contohnya adalah seseorang yang melakukan DoS pada mesin ATM. Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Sebagai akibatnya, maka nasabah bank tidak bisa melakukan transaksi sehingga bank akan mengalami kerugian finansial. DoS attack ditujukan kepada server dan juga ditargetkan pada jaringan yang dapat menghabiskan *bandwidth*.

j. Cybersquatting and Typosquatting

Cybersquatting merupakan jenis kejahatan yang dapat dilakukan dengan cara mendaftarkan domain sebuah nama perusahaan, kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Nama domain adalah nama yang biasanya digunakan oleh pemakai layanan www (world wide web) pada jaringan Internet dengan tujuan mengidentifikasi perusahaan dan merek dagang yang dimilikinya. Kesempatan semacam ini seringkali dimanfaatkan oleh orang untuk mendapatkan keuntungan dengan cara mendaftarkan nama domain perusahaan orang lain dan kemudian menjualnya dengan harga yang lebih mahal. Aktivitas semacam ini seperti seorang calo karcis. Adapun *typosquatting* merupakan jenis kejahatan yang dilakukan dengan membuat domain plesetan di mana domain tersebut mirip dengan nama domain orang lain. Contohnya adalah nama domain yang merupakan nama domain saingan perusahaan. Salah satu kasus yang pernah terjadi pada tahun 2000-an adalah kasus pemalsuan situs web bank BCA. Sang pelaku membeli beberapa nama domain plesetan dari kemungkinan ketidaksadaran nasabah melakukan *typo*. Lalu, si pelaku membuat duplikat situs web bank BCA dengan harapan nasabah tidak sadar jika mereka melakukan kesalahan pengetikan domain. Beberapa contoh nama domain yang dibeli adalah www.clickbca.com, www.kilkbca.com, www.kliklbca.com, dan variasi lainnya.

k. Hijacking

Hijacking adalah kejahatan dengan melakukan pembajakan hasil karya orang lain. Kejahatan yang paling sering terjadi adalah *Software Piracy* (pembajakan perangkat lunak). Merebaknya pembajakan pada jaringan Internet tersebut dipacu oleh sifat keluwesan yang dimiliki Internet itu sendiri. Harus diakui bahwa teknologi Internet khususnya atau teknologi digital pada umumnya bersifat luwes. Artinya, apabila informasi yang tersedia berbentuk digital maka tanpa kesulitan seseorang dapat menyalinnya kemudian membagikannya kepada orang lain. Itu artinya bahwa segala sesuatu yang disediakan pada jaringan Internet dapat mempermudah orang dalam mengutip serta menggunakannya tanpa seijin pemiliknya.

l. Cyber terorism

Merupakan sebuah tindakan *cybercrime* yang termasuk *cyber terorism* apabila mereka mengancam pemerintah serta warga negaranya. Salah satu contohnya adalah *cracking* ke situs pemerintah atau militer. Pemilihan teknologi informasi dalam melakukan kejahatan terorisme merupakan alasan yang tepat dipilih oleh teroris untuk melakukan komunikasi dengan aman.

2. Berdasarkan Motif Kegiatannya

Terdapat dua jenis motif kegiatan yang dilakukannya pada kejahatan siber, yaitu:

a. Cybercrime sebagai tindakan murni criminal

Kejahatan yang dilakukan dengan alasan melakukan kejahatan merupakan kejahatan dengan motif kriminalitas. Internet merupakan sarana kejahatan utama yang digunakan oleh pelaku kejahatan ini. Terdapat beberapa jenis kejahatan ini, salah satunya adalah *carding*. *Carding* merupakan sebuah kejahatan yang dilakukan dengan melakukan pencurian nomor kartu kredit milik orang lain agar dapat digunakan dalam melakukan transaksi perdagangan Internet.

Contoh kejahatan dengan pemanfaatan media Internet juga dilakukan dengan menyebarkan material bajakan. Pengiriman email anonim dengan mempromosikan sesuatu (*spamming*). Di beberapa negara tindak kejahatan *spamming* diberikan tuntutan dengan tuduhan pelanggaran privasi orang lain.

b. Cybercrime sebagai kejahatan "abu-abu"

Tindakan jenis ini sangat sulit untuk diidentifikasi karena kejahatan ini merupakan tindak kejahatan yang motifnya bukan kriminal. Salah satu contohnya adalah *probing* atau *port scanning*. Kejahatan ini merupakan sebuah tindakan pengintaian terhadap sistem milik orang lain. Pengumpulan informasi sebanyak-banyaknya dengan cara mengintai sistem dan operasi yang dilakukan, port-port yang ada, baik yang terbuka maupun yang tertutup.

Pada jenis kejahatan ini, pelaku kejahatan tidak melakukan tindakan apapun terhadap sistem yang diintainya, akan tetapi ia mendapatkan sesuatu yang sangat bermanfaat untuk melakukan aksi sesungghnya yang mungkin destruktif. Juga termasuk ke dalam "wilayah abu-abu" ini adalah kejahatan yang berhubungan dengan nama domain di Internet. Banyak orang yang melakukan semacam kegiatan "percaloan" pada nama domain dengan membeli domain yang mirip dengan merek dagang atau nama perusahaan tertentu dan kemudian menjualnya dengan harga tinggi kepada pemilik merek atau perusahaan yang bersangkutan. Kegiatan ini diistilahkan sebagai *cybersquatting*. Kegiatan lain yang hampir mirip dikenal sebagai *typosquatting*, yaitu membuat nama domain "plesetan" dari domain yang sudah popular. Para pelaku *typosquatting* berharap dapat mengeruk keuntungan dari pengunjung yang tersasar ke situsnya karena salah mengetik nama domain yang dituju pada browsernya.

3. Berdasarkan Sasaran Kejahatannya

Jenis kejahatan yang dilihat berdasarkan sasaran kejahatannya dapat dibedakan menjadi beberapa jenis di antaranya:

a. Cybercrime yang menyerang individu (against person)

Jenis kejahatan ini dilakukan dengan sasaran korbannya adalah perorangan. Kejahatan ini dilakukan untuk sekedar melakukan penyerangan terhadap seseorang dengan sikap atau kriteria tertentu. Berikut merupakan contoh jenis kejahatan yang menyerang individu:

1) Pornografi

   Merupakan kejahatan siber yang dilakukan dengan membuat, memasang, mendistribusikan dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas ke dunia maya dengan tujuan yang tidak jelas.

2) *Cyberstalking*

   Merupakan jenis kejahatan yang dilakukan dengan tujuan untuk mengganggu atau melecehkan seseorang melalui pemanfaatan media komputer. Contohnya adalah tindakan kejahatan dengan menggunakan e-mail. Penggunaan e-mail tersebut dilakukan secara berulang-ulang seperti sebuah teror di dunia kejahatan maya. Gangguan tersebut bisa saja berbau seksual, rasial, religius, dan lain sebagainya.

3) *Cyber-Tresspass*

   Kejahatan *cyber* yang dilakukan dengan melanggar area privasi seseorang, misalnya *web hacking, breaking* ke PC, *probing*, *port scanning*, dan lain sebagainya.

b. *Cybercrime menyerang hak milik (against property)*

Jenis kejahatan ini merupakan kejahatan yang dilakukan dengan mengganggu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia siber, pemilikan informasi elektronik secara ilegal, melakukan pencurian informasi atau *carding, cybersquatting, typosquatting,* dan *hijacking,* serta *data forgery* atau pemalsuan data yang dapat merugikan orang lain.

c. *Cybercrime menyerang pemerintah (against government)*

Cybercrime against government merupakan aktivitas tindak kejahatan siber dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya *cyberterrorism* sebagai tindakan yang mengecam pemerintah termasuk juga cracking ke situs resmi pemerintah atau situs militer.

D. TIPE-TIPE ANCAMAN SIBER

Ancaman (*threat*) yang menjadi lawan para *cyber-security* setidaknya ada tiga pihak, yaitu:

1. *Cybercrime* (kejahatan siber) mencakup pelaku tunggal atau kelompok yang menargetkan sistem untuk keuntungan finansial atau menyebabkan gangguan.
2. *Cyber-attack* (serangan siber) sering kali melibatkan pengumpulan informasi yang bermotivasi politik.
3. *Cyberterrorism* (teroris siber) dimaksudkan untuk merusak sistem elektronik yang menyebabkan kepanikan atau ketakutan.

Lalu bagaimana para aktor jahat (*malicious actors*) mendapatkan kendali atas sistem komputer dan jaringan termasuk Internet? Berikut beberapa metode umum yang digunakan untuk mengancam keamanan siber (*cyber-security*):

1. Malware

Malware merupakan sebuah istilah metode yang digunakan untuk mengancam keamanan siber. Malware merupakan kependekan dari **mal**icious soft**ware** (perangkat lunak berbahaya) dan merupakan salah satu ancaman siber yang paling umum. Malware merupakan perangkat lunak yang dibuat oleh penjahat siber (*cybercriminal*) atau peretas (*hacker*) untuk mengganggu atau merusak komputer pengguna yang sah (*legitimate users*). Malware seringkali menyebar melalui lampiran email (*email attachment*) yang tidak diminta atau unduhan yang tampak sah. Malware sangat dimungkinkan juga untuk digunakan oleh penjahat siber untuk menghasilkan uang atau untuk serangan siber yang bermotif politik. Ada beberapa jenis malware di antaranya:

a. **Virus** merupakan sebuah program untuk menggandakan diri-sendiri dan menempel pada file yang bersih serta menyebar ke seluruh bagian sistem komputer. Virus kemudian menginfeksi file dengan menggunakan kode berbahaya (*malicious code*) yang menyebabkan jaringan komputer menjadi lumpuh.
b. **Trojans** merupakan tipe malware yang menyamar dalam bentuk perangkat lunak yang sah. Hal ini dilakukan oleh penjahat siber (*cybercriminals*) dengan menipu pengguna untuk mengunggah Trojan pada jaringan komputer mereka. Hal tersebut menyebabkan kerusakan dalam mengumpulkan data.
c. **Spyware** merupakan sebuah program yang dengan diam-diam merekam segala kegiatan yang dilakukan oleh pengguna. Kemudian semua informasi yang diperoleh digunakan untuk tindak

kejahatan. Contohnya adalah mengambil informasi dalam kartu kredit serta menggunakannya untuk kepentingan pelaku kejahatan.

d. **Ransomware** merupakan sebuah malware yang bekerja dengan mengunci file serta data yang disimpan oleh pengguna. Kejahatan ini dilakukan dengan memberi sebuah ancaman menghapus data pemiliknya dengan meminta tebusan berupa uang.
e. **Adware** merupakan sebuah software periklanan. Software ini digunakan untuk menyebarkan malware.
f. **Botnet** merupakan jaringan komputer yang terinfeksi malware yang digunakan penjahat siber untuk melakukan tugas secara online tanpa izin pengguna.

2. *Structured Query Language* (SQL) injection (Injeksi pada SQL)

Structured Query Language (SQL) injection atau injeksi bahasa kueri terstruktur merupakan sebuah serangan siber yang dilakukan guna mengambil kendali dan mencuri data dari basisdata. Penjahat siber mengeksploitasi kerentanan dalam aplikasi berbasis data untuk memasukkan kode berbahaya (*malicious code*) ke dalam basisdata melalui pernyataan SQL yang berbahaya (*malicious* SQL *statement*). Ini memberikan mereka akses ke informasi sensitif yang terkandung dalam database.

3. *Phishing*

Phishing merupakan situasi di mana penjahat siber memiliki target korban kejahatan yang akan dilakukannya. Ia melakukan pengiriman email dengan meminta informasi penting terkait perusahan yang menjadi korbannya. Serangan phishing sering kali digunakan untuk menipu orang agar menyerahkan data kartu kredit dan informasi pribadi lainnya.

4. *Man-in-the-Middle* (MiM) *Attack*

Serangan *man-in-the-middle* adalah jenis ancaman siber (*cyber threats*) di mana penjahat siber menyadap komunikasi antara dua individu untuk mencuri data. Misalnya, pada jaringan WiFi yang tidak aman, penyerang dapat mencegat data yang dikirimkan dari perangkat korban dan jaringan.

4. *Denial-of-Service* (DoS) *Attack*

Merupakan sebuah serangan berupa penolakan layanan (*denial-of-service*) yaitu ketika penjahat siber melakukan pencegahan terhadap sistem komputer memenuhi permintaan yang sah dengan membanjiri jaringan dan server dengan lalu lintas. Ini membuat sistem tidak dapat digunakan, mencegah organisasi menjalankan fungsi vital.

E. KIAT-KIAT KEAMANAN SIBER

Terdapat beberapa cara untuk melakukan keamanan siber, salah satunya adalah dengan melakukan pembaruan (*update*) pada celah keamanan dengan cara menginstal *security patches* terbaru. Berikut beberapa kiat yang dapat dilakukan untuk mengamankan siber, di antaranya adalah:

1. menggunakan perangkat lunak anti-virus: solusi keamanan seperti McAfee, Kaspersky, Defender, AVG, dan anti-virus lainnya akan mendeteksi dan menghapus ancaman. Selalu perbarui perangkat lunak Anda untuk meningkatkan perlindungan terbaik.
2. menggunakan kata sandi yang kuat (*strong password*): Pastikan kata sandi Anda tidak mudah ditebak. Beberapa aplikasi seperti Google, Apple, dan Microsoft merekomendasikan panjang password minimal 8 karakter dengan kombinasi angka, huruf, dan spesial karakter. Bahkan saat

ini ketiganya telah menerapkan 2-steps *verification* atau menerapkan pembangkit kunci (*key generator*).

3. jangan membuka lampiran email dari pengirim yang tidak dikenal. Hal ini dikarenakan ada kemungkinan terinfeksi malware.
4. jangan menekan (klik) tautan dalam email dari pengirim tak dikenal atau situs web tak dikenal. Cara ini adalah cara umum penyebaran perangkat lunak jahat (*malicious software/malware*).
5. hindari menggunakan jaringan WiFi yang tidak aman di tempat umum. Jaringan yang tidak aman (*unsecure networks*) membuat Anda rentan terhadap serangan *man-in-the-middle*. Biasanya, WiFi yang diakses tidak menggunakan metode enkripsi.

F. METODE KEJAHATAN CYBERCRIME

Dengan semakin banyaknya kejahatan di dunia maya saat ini maka terdapat beragam metode yang dilakukan untuk melakukan kejahatan tersebut. Berikut ini adalah beberapa cara kerja *cybercrime* yang sering dilakukan:

1. *Password Cracker*

Tindakan ini merupakan tindakan pencurian password orang lain dengan menggunakan sebuah program yang dapat membuka enkripsi password. Tindakan ini juga sering dilakukan untuk menonaktifkan suatu sistem pengamanan password.

2. *Spoofing*

Spoofing merupakan sebuah tindakan kejahatan siber dengan memalsukan data atau identitas seseorang. Dalam hal ini pelaku kejahatan dapat login ke dalam sebuah jaringan komputer layaknya pengguna aslinya.

3. DDoS (*Distributed Denial of Service Attacks*)

Merupakan serangan yang dilakukan pada sebuah komputer atau server di dalam jaringan Internet yang dilakukan oleh seorang *hacker/attacker*. Serangan *DDoS* akan menghabiskan sumber daya (*resource*) yang ada pada suatu komputer atau server hingga tidak dapat lagi menjalankan fungsinya dengan benar.

4. *Sniffing*

Sniffing merupakan bentuk kejahatan siber di mana pelaku mencuri username dan password orang lain secara sengaja maupun tidak sengaja. Pelaku kemudian dapat memakai akun korban untuk melakukan penipuan atas nama korban atau merusak/menghapus data milik korban.

5. *Destructive Devices*

Merupakan sebuah program atau software berisi virus di mana tujuannya adalah untuk merusak atau menghancurkan data-data di dalam komputer korban. Beberapa yang termasuk dalam program ini adalah Worms, Trojan Horse, Nukes, Email Bombs, dan lain-lain.

G. PENANGGULANGAN *CYBERCRIME*

Aktivitas pokok dari *cybercrime* adalah penyerangan terhadap konten, sistem komputer, dan sistem komunikasi (jaringan komputer) milik pihak lain baik individu maupun organisasi di dalam *cyberspace*. Fenomena *cybercrime* memang harus diwaspadai karena kejahatan ini agak berbeda

dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global *Internet*, semua negara yang memerlukan kegiatan Internet akan terkena potensi serangan dari *cybercrime* ini.

Berikut akan dibahas beberapa hal pokok yang dapat dilakukan dalam upaya menanggulangi merebaknya kejahatan Internet:

1. Mengamankan Sistem

Tujuan utama pengamanan sebuah sistem untuk mencegah adanya perusakan bagian sistem jaringan komputer. Oleh karena itu, sistem yang dibangun harus terintegrasi pada seluruh bagian sistemnya. Hal ini dilakukan untuk menutup dan meminimalkan celah yang dapat merugikan pemiliknya. Pengamanan yang dilakukan bisa berupa pengamanan personal di mana setiap tahapan bertujuan untuk menjaga keamanan sistem komputer. Pengamanan dilakukan dengan menginstalas sistem hingga pengamanan data. Dalam hal ini pengamanan dilakukan pada pengamanan FTP, SMTP, Telnet, dan pengamanan Web Server.

2. Penanggulangan Global

Terdapat beberapa langkah yang harus diambil oleh suatu negara untuk menanggulangi kejahatan siber yang makin marak saat ini. Di antaranya adalah dengan melakukan modernisasi hukum pidana nasional beserta hukum acaranya; 2) melakukan peningkatan sistem jaringan sesuai dengan sistem jaringan internasional; 3) meningkatkan pemahaman aparatur penegak hukum mengenai pencegahan dan investigasi perkara mengenai kejahatan siber; 4) meningkatkan kesadaran warga negara mengenai kejahatan siber serta; 5) melakukan peningkatan kerjasama antar negara.

3. Langkah untuk Keamanan Siber

Pendekatan yang efektif untuk keamanan siber (*cyber security*) dimulai dengan menetapkan rezim manajemen risiko organisasi yang efektif seperti ditunjukkan pada **Error! Reference source not found.**.

a. Rezim manajemen risiko (risk management regime)

Kunci dari manajemen ini adalah menanamkan rezim manajemen risiko yang sesuai di seluruh organisasi haruslah didukung oleh struktur tata kelola yang diberdayakan yang secara aktif didukung oleh Dewan Direksi dan Manajer Senior. Komunikasikan secara jelas pendekatan Anda terhadap manajemen risiko dengan pengembangan kebijakan dan praktik yang berlaku. Ini harus bertujuan untuk memastikan bahwa semua karyawan, kontraktor, dan pemasok mengetahui pendekatan, bagaimana keputusan dibuat, dan batasan risiko yang berlaku.

b. Konfigurasi aman (secure configuration)

Terapkan *patch* keamanan, dan pastikan konfigurasi aman dari semua sistem dipertahankan. Buatlah inventaris sistem dan tentukan bangunan dasar (*baseline*) untuk semua perangkat.

c. Keamanan jaringan (network security)

Lindungi jaringan Anda dari serangan. Pertahankan perimeter jaringan, saring akses tidak sah dan konten berbahaya. Monitor dan uji kontrol keamanan.

d. Mengelola hak istimewa pengguna (managing user privileges)

Tetapkan proses manajemen yang efektif dan batasi jumlah akun yang memiliki hak istimewa. Batasi hak istimewa pengguna dan pantau aktivitas pengguna. Kontrol akses ke aktivitas dan log audit.

e. Pendidikan dan kesadaran pengguna (user education and awareness)

Menghasilkan kebijakan keamanan pengguna yang mencakup penggunaan sistem Anda yang dapat diterima dan aman. Sertakan aspek ini dalam pelatihan staf. Pertahankan kesadaran akan risiko siber.

f. Manajemen insiden (incident management)

Membangun kemampuan tanggap (respon) insiden dan pemulihan bencana (*disaster recovery*). Uji rencana manajemen insiden Anda. Berikan pelatihan spesialis. Laporkan insiden kriminal kepada penegak hukum.

g. Pencegahan malware (malware prevention)

Buatlah kebijakan yang relevan dan buat pertahanan anti-malware di seluruh organisasi Anda.

h. Pemantauan (monitoring)

Menetapkan strategi pemantauan dan menghasilkan kebijakan pendukung. Terus pantau semua sistem dan jaringan. Analisis log untuk aktivitas tidak biasa yang dapat mengindikasikan serangan.

i. Kontrol media yang dapat dilepas (removable media controls)

Buatlah kebijakan untuk mengontrol semua akses ke media yang dapat dilepas. Batasi jenis dan penggunaan media. Pindai semua media untuk mencari malware sebelum mengimpor ke sistem perusahaan.

j. Pekerjaan rumah dan mobile (home and mobile working)

Kembangkan kebijakan kerja *mobile* dan latih staf untuk mematuhinya. Terapkan garis dasar yang aman dan buat ke semua perangkat. Lindungi data saat transit dan saat istirahat.

4. Beberapa Contoh Kasus Cybercrime yang Terjadi di Masyarakat

a. Kasus 1: Perdagangan Brownies Berbahan Ganja melalui Online

Pada bulan April lalu BNN berhasil menangkap sindikat pembuat brownies berbahan ganja di kawasan Blok M Plaza dengan tersangka sebanyak 5 orang. Pengungkapan kasus tersebut berawal dari laporan masyarakat, yakni seorang siswa SMP yang tertidur 2 hari 2 malam setelah mengkonsumsi kue brownies atau coklat tersebut. Usut punya usut ternyata anak tersebut tidur setelah makan brownies yang mengandung ganja. Kasus tersebut merupakan modus paling baru dari perwujudan narkotika, yaitu untuk penjualan kue dan coklat yang mengandung ganja dilakukan secara online melalui website dan untuk mendapatkan kue tersebut para konsumen memesan via telepon dan BBM.

> "Tersangka dikenakan Pasal 111 ayat 2, dan Pasal 114 ayat 2 No. 132 UU No. 35/2009 tentang narkotika dengan ancaman hukuman maksimal pidana mati atau penjara seumur hidup"

b. Kasus 2: Penipuan Tiket via Internet

Pada tahun 2013 marak terjadinya penipuan yang disebarluaskan melalui SMS. Salah satu pelaku yang tertangkap adalah enam tersangka yang juga terlibat penjualan senjata online. Modus yang dilakukan yakni menawarkan tiket murah melalui penyebaran SMS melalui www.smscaster.com dan

memasukkan nomor acak per hari mencapai 3000 nomor. Dari nomor-nomor itu, kadang kala ada 5-10 nomor calon korban yang akan menghubungi. Rikwanto menambahkan, per harinya komplotan ini bisa meraup untung sekitar Rp600.000 sampai Rp10.000.000, dan pelaku sudah melakukan aksinya sejak 2010 lalu.

> "Penyelesaiannya: Pelaku dapat dijerat dengan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, maka pasal yang dikenakan adalah Pasal 28 ayat (1), yang berbunyi sebagai berikut: "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik". Dengan ancaman pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1 miliar (Pasal 45 ayat [2] UU ITE). Untuk pembuktiannya, APH bisa menggunakan bukti elektronik dan/atau hasil cetaknya sebagai perluasan bukti sebagaimana Pasal 5 ayat (2) UU ITE, di samping bukti konvensional lainnya sesuai dengan Kitab Undang-Undang Hukum Acara Pidana (KUHAP)"

H. *CYBER LAW*

Cyberlaw merupakan sebuah hukum dunia maya, yang umumnya diasosiasikan dengan jaringan Internet. *Cyberlaw* dibutuhkan karena dasar atau fondasi dari hukum di banyak negara adalah "ruang dan waktu". Sementara itu, Internet dan jaringan komputer merupakan fasilitas yang mampu menerobos batas ruang dan waktu ini.

Beberapa contoh permasalahan yang berhubungan dengan hilangnya ruang dan waktu antara lain:

1. Seorang penjahat komputer (*cracker*) yang berkebangsaan Indonesia, berada di Australia, mengobrak-abrik server di Amerika, yang ditempati (*hosting*) sebuah perusahaan Inggris. Hukum mana yang akan dipakai untuk mengadili kejahatan *cracker* tersebut? Contoh kasus yang mungkin berhubungan adalah *hacker* Indonesia yang tertangkap di Singapura karena melakukan *cracking* terhadap sebuah server perusahaan di Singapura. Dia diadili dengan hukum Singapura karena kebetulan semuanya berada di Singapura.
2. Nama domain (.com, .net, .org, .id, .sg, dan seterusnya) pada mulanya tidak memiliki nilai apa-apa. Akan tetapi dengan perkembangan Internet, nama domain adalah identitas dari perusahaan. Bahkan karena dominannya perusahaan Internet yang menggunakan domain ".com" sehingga perusahaan-perusahaan tersebut sering disebut perusahaan "dotcom". Pemilihan nama domain sering berbenturan dengan trademark, nama orang terkenal, dan seterusnya. Contoh kasus adalah pendaftaran domain JuliaRoberts.com oleh orang yang bukan Julia Roberts (akhirnya pengadilan memutuskan Julia Roberts yang asli yang menang). Adanya perdagangan global, WTO, WIPO, dan lain lain, membuat permasalahan menjadi semakin keruh. Trademark menjadi global.
3. Pajak (*tax*) juga merupakan salah satu masalah yang cukup pelik. Dalam transaksi yang dilakukan oleh multi nasional, pajak mana yang akan digunakan? Seperti contoh di atas, server berada di Amerika, dimiliki oleh orang Belanda, dan pembeli dari Rusia. Bagaimana dengan pajaknya? Apakah perlu dikenakan pajak? Ada usulan dari pemerintah Amerika Serikat di mana pajak untuk produk yang dikirimkan (*delivery*) melalui saluran Internet tidak perlu dikenakan pajak. Produk-produk ini biasanya dikenal dengan istilah "digitalized products", yaitu produk yang dapat di-digital-kan, seperti musik, film, software, dan buku. Barang yang secara fisik dikirimkan secara konvensional dan melalui pabean, diusulkan tetap dikenakan pajak.
4. Bagaimana status hukum dari uang digital seperti *cybercash*? Siapa yang boleh menerbitkan uang digital ini?

   Perkembangan teknologi komunikasi dan komputer sudah demikian pesatnya sehingga mengubah pola dan dasar bisnis. Untuk itu *cyberlaw* ini sebaiknya dibahas oleh orang-orang dari berbagai latar belakang (akademisi, pakar TekInfo, teknis, hukum, bisinis, dan pemerintah). Munculnya kejahatan di Internet pada awalnya banyak menimbulkan pro-kontra terhadap

penerapan hukum yang harus dilakukan. Hal ini dikarenakan saat itu sulit untuk menjerat hukum para pelakunya karena beberapa alasan. Alasan yang menjadi kendala seperti sifat kejahatannya bersifat maya, lintas negara, dan sulitnya menemukan pembuktian.

Semua orang akan sependapat (kesepakatan universal) bahwa segala bentuk kejahatan harus dikenai sanksi hukum, menurut kadar atau jenis kejahatannya. Begitu juga kejahatan TI apapun bentuknya tergolong tindakan kejahatan yang harus dihukum. Pertanyaan yang sering diajukan adalah apakah perundangan di Indonesia sudah mengatur masalah tersebut? Wigrantoro dalam naskah akademik tentang RUU bidang TI menyebutkan terdapat dua kelompok pendapat dalam menjawab pertanyaan ini:

1. **Kelompok pertama** berpendapat bahwa hingga saat ini belum ada perundangan yang mengatur masalah kriminalitas penggunaan TI (*cybercrime*) dan oleh karena itu jika terjadi tindakan kriminal di dunia maya sulit bagi aparat penegak hukum untuk menghukum pelakunya. Pendapat ini diperkuat dari kenyataan bahwa banyak kasus kriminal yang berkaitan dengan dunia maya tidak dapat diselesaikan oleh sistem peradilan dengan tuntas karena aparat menghadapi kesulitan dalam melakukan penyidikan dan mencari pasal-pasal hukum yang dapat digunakan sebagai landasan tuntutan di pengadilan.
2. **Kelompok kedua** beranggapan bahwa tidak ada kekosongan hukum, oleh karenanya meski belum ada undang-undang yang secara khusus mengatur masalah *cybercrime*, para penegak hukum dapat menggunakan ketentuan hukum yang sudah ada. Untuk melaksanakannya diperlukan keberanian hakim menggali dari undang-undang yang ada dan membuat ketetapan hukum (yurisprudensi) sebagai landasan keputusan pengadilan. Kelompok ini berpendapat bahwa mengingat lamanya proses penyiapan suatu undang-undang, sementara demi keadilan, penanganan tindakan kejahatan TI tidak dapat ditunda, maka akan lebih baik kiranya jika digali ketentuan hukum yang ada dan dianalisis apakah ketentuan hukum tersebut dapat digunakan sebagai landasan tuntutan dalam kejahatan TI.

Pendapat dua kelompok di atas mendorong diajukannya tiga alternatif pendekatan dalam penyediaan perundang-undangan yang mengatur masalah kriminalitas TI, yaitu:

1. Alternatif Pertama, dibuat undang-undang khusus yang mengatur masalah tindak pidana di bidang TI. Undang-undang ini bersifat *lex specialist* yang khusus mengatur masalah pidana pelanggaran pemanfaatan TI, baik yang tergolong kajahatan konvensional menggunakan komputer sebagai alat, maupun kejahatan jenis baru yang muncul setelah adanya Internet dan menjadikan TI sebagai sarana kejahatan.
2. Alternatif kedua, memasukkan materi kejahatan TI ke dalam amandemen KUHP yang digodok oleh tim Departemen Kehakiman dan HAM. Sebagai mana diketahui KUHP belum mencakup jenis-jenis kejahatan TI, khususnya di dunia maya.
3. Alternatif ketiga, melakukan amandemen terhadap semua undang-undang yang diperkirakan akan berhubungan dengan pemanfaatan TI, seperti misalnya UU perpajakan, perbankan, asuransi, kesehatan, pendidikan nasional, dan lain-lain. Amandemen terhadap berbagai UU ini untuk menyesuaikan kemungkinan adanya pelanggaran terhadap klausa yang tergolong pidana.

Sekarang ini negara kita sudah memiliki Undang-undang Informasi dan Transaksi Elektronik (UU ITE) yang merupakan salah satu perangkat hukum untuk mengatur pemanfaatan TI. Di samping itu negara RI perlu juga memiliki Undang-undang Tindak Pidana di Bidang Teknologi Informasi (UU TIPITI). Diharapkan kedua undang-undang ini dapat saling melengkapi dalam memberikan kepastian dan perlindungan hukum bagi masyarakat pengguna TI.

Upaya yang dilakukan pemerintah dalam rangka memberikan payung hukum ruang cyber dengan mengesahkan Undang-undang Informasi dan Transaksi Elektronik (UU No. 11 th 2008 tentang ITE) pada tanggal 21 April 2008. UU ITE memuat beberapa hal yakni: masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara e-commerce, azas persaingan usaha tidak sehat, dan perlindungan konsumen, azas-azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional, serta azas *cybercrime*.

Dalam Undang-Undang ini pada **Pasal 1** yang dimaksud dengan:

1. **Informasi Elektronik** adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
2. **Transaksi Elektronik** adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.
3. **Teknologi Informasi** adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
4. **Dokumen Elektronik** adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makan atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
5. **Sistem Elektronik** adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

Dalam **Pasal 2** mengungkapkan Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia tentang Informasi dan Transaksi Elektronik (ITE) pada **Pasal 3** terdiri atas asas-asas sebagai berikut:

1. Asas Kepastian Hukum
2. Asas Manfaat
3. Asas kehati-hatian
4. Asas iktikad baik
5. Asas kebebasan memilih teknologi atau netral teknologi

Pasal 4 berbicara tentang pemanfaatan Teknologi Informasi dan Transaksi Elektronik. **Pasal 5** mengatur bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia sesuai dengan ketentuan yang diatur dalam Undang-Undang ini, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan **(Pasal 6),** dan setiap orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik

yang memenuhi syarat berdasarkan Peraturan Perundang-undangan **(Pasal 7)** untuk waktu pengiriman dan penerimaan yang diatur pada **Pasal 8**.

Sementara itu, bagi pelaku usaha yang menawarkan produk melalui Sistem Elektronik ada pula payung hukumnya. Yakni, harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan. Hal itu diatur dalam **Pasal 9**. Sertifikasi keandalan dapat dilakukan oleh lembaga Sertifikasi Keandalan untuk setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik **(Pasal 10),** sedangkan pengaturan terkait tanda tangan elektronik dan penyelenggara sertifikasi elektronik diatur dalam **Pasal 11-14.** Untuk Pengaturan tentang Penyelenggaraan Sistem Elektronik diatur pada **Pasal 15-16**, sedangkan **Pasal 17- 22** mengatur tentang transaksi elektronik dan hal-hal yang terkait dengan transaksi elektronik.

Tak hanya itu, penjelasan mengenai nama domain, hak kekayaan intelektual, dan perlindungan hak pribadi sudah tercantum dalam UU ini, tepatnya **Pasal 23**. Pada **Pasal 23 Ayat 1** membolehkan setiap penyelenggara negara, orang, Badan Usaha, dan/atau masyarakat untuk memiliki Nama Domain berdasarkan prinsip pendaftar pertama.

Untuk Pengelola Nama Domain yang berada di luar wilayah Indonesia dan Nama Domain yang diregistrasinya diakui keberadaannya sepanjang tidak bertentangan dengan Peraturan Perundang-undangan (**Pasal 24**). Demikian penjelasan dari beberapa pasal-pasal dalam UU ITE dan masih banyak lagi pasal-pasal dalam UU ITE lebih kurang sekitar 52 pasal.

Hukum komunikasi adalah praktik hukum yang berkaitan dengan pertukaran informasi dengan menggunakan teknologi. Itu adalah hukum apa pun yang melibatkan pengaturan dan penggunaan telekomunikasi elektronik. Hukum komunikasi mencakup teknologi seperti radio, televisi, kabel dan Internet broadband. Ini melibatkan pembuatan aturan dan kebijakan yang mengatur penggunaan teknologi ini. Peraturan komunikasi mengatur komunikasi publik dan pribadi. Anggota parlemen membuat peraturan ini dengan tujuan membuat teknologi komunikasi dapat diakses oleh semua orang Amerika dengan harga yang wajar. Sebagian besar undang-undang dan peraturan komunikasi di Amerika Serikat melibatkan badan federal Komisi Komunikasi Federal (*Federal of Communication Commission*, FCC).