Jurnal TIMES , Vol. V No 2 : 35-42 , 2016
ISSN : 2337 - 3601

CYBERCRIME, CYBER SPACE, DAN *CYBER LAW*

Eliasta Ketaren
STMIK TIME
Jl. Merbabu No. 32 AA-BB, Medan 20212
e-mail : eliastaketaren@yahoo.com

Abstrak

Pemanfaatan dalam bidang teknologi Informasi, media, dan komunikasi telah membuat perilaku seseorang menjadi lebih baik dalam berperilaku dalam sebuah masyarakat. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tidak terhalang dengan batas dan norma yang ada sehingga dapat menimbulkan suatu perubahan dalam seluruh bidang missal bidang sosial, ekonomi, dan budaya secara cepat dan luas. Teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi factor penting dalam perbuatan melawan hukum. Perubahan ini juga memberikan dampak yang begitu besar terhadap transformasi nilai-nilai yang ada di masyarakat. Dampak yang ditimbulkan dari perkembangan teknologi bukan hanya dampak positif namun ada dampak negatif, perkembangan teknologi yang dimanfaatkan untuk tindak kejahatan yang biasa dikenal dengan cybercrime. Cybercrime mengacu kepada aktifitas kejahatan dengan komputer atau jaringan komputer yang menjadi alat atau tempat terjadinya kejahatan. Beberapa contoh dari cybercrime antara lain hacking, cracking, defacing, dll. Begitu juga dengan pembobolan ATM, judi online, dan pornografi termasuk dalam kejahatan dengan komputer.

Kata Kunci : Cybercrime, Hacking, Cracking, Cyber Space, Cyber Law

1. Pendahuluan

Kebutuhan akan teknologi Jaringan Komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui Internet pula kegiatan komunitas komersial menjadi bagian terbesar, dan terpesat pertumbuhannya serta menembus berbagai batas negara. Bahkan melalui jaringan ini kegiatan pasar di dunia bisa diketahui selama 24 jam. Melalui dunia internet atau disebut juga cyber space, apapun dapat dilakukan. Segi positif dari dunia maya ini tentu saja menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Namun dampak negatif pun tidak bisa dihindari. Tatkala pornografi marak di media Internet, masyarakat pun tak bisa berbuat banyak.

Seiring dengan perkembangan teknologi Internet, menyebabkan munculnya kejahatan yang disebut dengan "Cybercrime" atau kejahatan melalui jaringan Internet. Munculnya beberapa kasus "Cybercrime" di Indonesia, seperti pencurian kartu kredit, hacking beberapa situs, menyadap transmisi data orang lain, misalnya email, dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programmer komputer. Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya Cybercrime telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

1.1. Maksud Dan Tujuan

Maksud penulisan makalah ini adalah:

1. Memenuhi salah satu tugas mata kuliah Keamanan Komputer
2. Menambah wawasan tentang Cybercrime
3. Sebagai masukan kepada mahasiswa agar menggunakan ilmu yang didapat untuk kepentingan yang positif

Tujuan penulisan makah ini adalah memberikan informasi tentang cybercrime kepada kami sendiri pada khususnya dan masyarakat yang membaca pada umumnya.

1.2. Manfaat

Manfaat penulisan makalah ini adalah agar pemahaman tentang tindak kejahatan melalui media internet dengan sebutan Cybercrime ini menjadi lebih mudah di mengerti bagi setiap orang yang membacanya. Dan khususnya untuk para pengguna media online, makalah ini merupakan informasi yang harus diaplikasikan dalam menggunakan media internet sebagai wadah untuk melakukan berbagai aktifitas dengan baik dan lebih hati-hati.

2. Landasan Teori

2.1. Sejarah Cybercrime

Cybercrime terjadi bermula dari kegiatan hacking yang telah ada lebih dari satu abad. Pada tahun 1870-an, beberapa remaja telah merusak sistem telepon baru Negara dengan merubah otoritas. Berikut akan ditunjukan seberapa sibuknya para hacker telah ada selama 35 tahun terakhir. Awal 1960 fasilitas universitas dengan kerangka utama computer yang besar, seperti laboratorium kepintaran buatan (artificial intel ligence) MIT, menjadi tahap percobaan bagi para hacker. Pada awalnya, kata " hacker" berarti positif untuk seorang yang menguasai computer yang dapat membuat sebuah program melebihi apa yang dirancang untuk melakukan tugasnya. Awal 1970 John Draper membuat sebuah panggilan telepon membuat sebuah

panggilan telepon jarak jauh secara gratis dengan meniupkan nada yang tepat ke dalam telepon yang memberitahukan kepada sistem telepon agar membuka saluran. Draper menemukan siulan sebagai hadiah gratis dalam sebuah kotak sereal anak-anak. Draper, yang kemudian memperoleh julukan "Captain Crunch" ditangkap berulangkali untuk pengrusakan telepon pada tahun 1970-an . pergerakan social Yippie memulai majalah YIPL/TAP (Youth International Party Line/ Technical Assistance Program) untuk menolong para hacker telepon (disebut "phreaks") membuat panggilan jarak jauh secara gratis. Dua anggota dari California's Homebrew Computer Club memulai membuat "blue boxes" alat yang digunakan untuk meng-hack ke dalam system telepon. Para anggotanya, yang mengadopsi pegangan "Berkeley Blue" (Steve Jobs) dan "Oak Toebark" (Steve Wozniak), yang selanjutnya mendirikan Apple computer. Awal 1980 pengarang William Gibson memasukkan istilah "Cyber Space" dalam sebuah novel fiksi ilmiah yang disebut Neurimancer. Dalam satu penangkapan pertama dari para hacker, FBI menggerebek markas 414 di Milwaukee (dinamakan sesuai kode area local) setelah para anggotanya menyebabkan pembobolan 60 komputer berjarak dari memorial Sloan-Kettering Cancer Center ke Los Alamos National Laboratory. Comprehensive Criem Contmrol Act memberikan yuridiksi Secret Service lewat kartu kredit dan penipuan computer. Dua bentuk kelompok hacker, The Legion of Doom di Amerika Serikat dan The Chaos Computer club di Jerman akhir 1980 penipuan computer dan tindakan penyalahgunaan member kekuatan lebih bagi otoritas federal Computer Emergency Response Team dibentuk oleh agen pertahanan Amerika Serikat bermarkas pada Carnegie Mellon University di Pittsburgh, misinya untuk menginvestigasi perkembangan volume dari penyerangan pada jaringan computer pada usianya yang ke 25,seorang hacker veteran bernama Kevin Mitnick secara rahasia memonitor email dari MCI dan pegawai keamanan digital equipment. Dia dihukum karena merusak computer dan mencuri software dan hal itu dinyatakan hukum selama satu tahun penjara.pada oktober 2008 muncul sesuatu virus baru yang bernama conficker (juga disebut down and up dan kido)yang terkatagori sebagai virus jenis worm.conficker menyerang windows dan paling banyak ditemui dalam windows XP. Microsoft merilis patch untuk menghentikan worm ini pada tanggal 15 oktober 2008. Heinz Haise memperkirakan conficker telah menginfeksi 2.5 juta PC pada 15 januari 2009, sementara the guardian memperkiran 3.5 juta PC terinfeksi. Pada 16 Januari 2009, worm ini telah menginfeksi hamper 9 juta PC, menjadikannya salah satu infeksi yang paling cepat menyebar dalam waktu singkat.

2.2. Definisi Cybercrime

Cybercrime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Beberapa pendapat mengindentikkan *cybercrime* dengan *computer crime*. **The U.S. Department of Justice** memberikan pengertien *computer crime* sebagai:

"…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution".

Pengertian tersebut identik dengan yang diberikan **Organization of European Community Development**, yang mendefinisikan *computer crime* sebagai:

"any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data".

Adapun Andi Hamzah (1989) dalam tulisannya "Aspek-aspek Pidana di Bidang komputer", mengartikan kejahatan komputer sebagai:

"Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal".

Dalam dua dokumen Kongres PBB mengenai The Prevention of Crime and the Treatment of Offenders di Havana, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal:

1. Cybercrime dalam arti sempit disebut computer crime, yaitu prilaku illegal atau melanggar secara langsung menyerang system keamanan suatu computer atau data yang diproses oleh komputer
2. Cybercrime dalam arti luas disebut computer related crime, yaitu prilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan

Dari beberapa pengertian diatas, secara ringkas dapat dikatakan bahwa cybercrime dapat didefinisikan adalah suatu tindakan kriminal yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat kejahatannya. Cybercrime ini terjadi karena ada kemajuan di bidang teknologi komputer atau dunia IT khususnya media internet.

Maraknya tindak kriminal di dunia maya tergantung dari sejauh mana sumber daya baik berupa hardware/software maupun pengguna teknologi yang bersangkutan mempunyai pengetahuan dan kesadaran tentang pentingnya keamanan di dunia maya, seorang penyedia layanan/target Cybercrime harus mempunyai pengetahuan yang cukup tentang metode yang biasanya seorang cybercrime lakukan dalam menjalankan aksinya.

3. Pembahasan

3.1. Karakteristik Cybercrime

Selama ini dalam kejahatan konvensional, dikenal adanya dua jenis kejahatan sebagai berikut:

1. Kejahatan Kerah Biru (Blue Collar Crime)
   Kejahatan ini merupakan jenis kejahatan atau tindak criminal yang dilakukan secara konvensional seperti misalnya perampokan, pencurian, pembunuhan,dll.
2. Kejahatan Kerah Putih (White Collar Crime)

Kejahatan jenis ini terbagi dalam empat kelompok kejahatan,yakni kejahatan korporasi, kejahatan birokrat, malpraktek, dan kejahatan individu.

Cybercrime sendiri sebagai kejahatan yang muncul sebagai akibat adanya komunitas dunia maya di internet, memiliki karakteristik tersendiri yang berbeda dengan kedua model diatas. Karakteristik unik dari kejahatan didunia maya tersebut antara lain menyangkut lima hal berikut :

1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Pelaku kejahatan
4. Modus kejahatan
5. Jenis-jenis kerugian yang ditimbulkan

Dari beberapa karakteristik diatas, untuk mempermudah penanganannya maka cybercrime dapat diklasifikasikan menjadi :

1. Cyberpiracy
   Penggunaan teknologi computer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau software tersebut lewat teknologi komputer.
2. Cybertrespass
   Penggunaan teknologi computer untuk meningkatkan akses pada system computer suatu organisasi atau indifidu.
3. Cybervandalism
   Penggunaan teknologi computer untuk membuat program yang menganggu proses transmisi elektronik, dan menghancurkan data dikomputer.

3.2. Jenis – Jenis Cybercrime

Berdasarkan motif kegiatannnya, cybercrime dapat digolongkan sebagai berikut:

1. Cybercrime sebagai tindakan kejahatan murni
   Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah Carding, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (webserver, mailing list) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (spamming) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku spamming dapat dituntut dengan tuduhan pelanggaran privasi.
2. Cybercrime sebagai tindakan kejahatan abu-abu
   Pada jenis kejahatan di internet yang masuk dalam wilayah ”abu-abu”, cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun tertutup, dan sebagainya.
3. Cybercrime yang menyerang individu (Againts Person)
   Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermaikan seseorang untuk mendapatkan kepuasan pribadi. Contoh : Pornografi, cyberstalking, dll
4. Cybercrime yang menyerang hak cipta / hak milik (Againts Property)
   Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi/umum ataupun demi materi/nonmateri.
5. Cybercrime yang menyerang pemerintah (Againts Government)
   Kejahatan yang dilakukan dengan pemerintah sebagai objek dengan motif melakukan terror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan system pemerintahan, atau menghancurkan suatu Negara (Cyber Terorism).

Berdasarkan modus atau jenis aktifitasnya cybercrime dapat digolongkan sebagai berikut:

1. Unauthorized Access
   Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.
2. Illegal Contents
   Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.
3. Penyebaran virus secara sengaja
   Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.
4. Data Forgery
   Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.
5. Cyber Espionage, Sabotage, and Extortion
   Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap

suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. Cyberstalking
   Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.
7. Carding
   Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.
8. Hacking dan Cracker
   Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.
9. Cybersquatting and Typosquatting
   Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.
10. Hijacking
    Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak).
11. Infringements of Privacy
    Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized,yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materilmaupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakittersembunyi dan sebagainya.
12. Offense against Intellectual Property
    Kejahatan ini ditujukan terhadap Hak atas Kekayaan Intelektual yang dimiliki pihak lain di internet. Sebagai contoh adalah peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
13. Defacing
    Defacing merupakan bagian dari kegiatan hacking web atau program application, yang menfokuskan target operasi pada perubahan tampilan dan/atau konfigurasi fisik dari web atau program aplikasi tanpa melalui source code program tersebut. Sedangkan deface itu sendiri adalah hasil akhir dari kegiatan cracking dan sejenisnya, tekniknya adalah dengan mebaca source codenya (ini khusus untuk konteks web hacking), kemudian mengganti image (misalnya), editing html tag dkk, dan lain-lain. Tindakan defacing ada yang semata-mata iseng, unjuk kebolehan, pamer kemampuan membuat program, tapi ada juga yang untuk mencuri data dan dijual kepada pihak lain.
14. Phising
    Phising merupakan kegiatan memancing pemakai komputer di internet (user) agar mau memberikan informasi data diri pemakai (username) dan kata sandinya (password) pada suatu website yang sudah di-deface. Phising biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya. Phising biasanya dilakukan melalui e-mail spoofing atau pesan instan, dan sering mengarahkan pengguna untuk memasukkan rincian di sebuah website palsu yang tampilan dan nuansa yang hampir sama dengan yang aslinya.
15. Spamming
    Spamming merupakan kegiatan mengirim email palsu dengan memanfaatkan server email yang memiliki “smtp open relay” atau spamming bisa juga diartikan dengan pengiriman informasi atau iklan suatu produk yang tidak pada tempatnya dan hal ini sangat mengganggu bagi yang dikirim. Yang paling banyak adalah pengiriman e-mail dapat hadiah, lotere, Kemudian korban diminta nomor rekeningnya, dan mengirim uang/dana sebagai pemancing, tentunya dalam mata uang dolar AS, dan belakangan tak ada kabarnya lagi.
16. Snooping
    Snooping adalah suatu pemantauan elektronik terhadap jaringan digital untuk mengetahui password atau data lainnya. Ada beragam teknik snooping atau juga dikenal sebagai eavesdropping, yakni: shoulder surfing (pengamatan langsung terhadap display monitor seseorang untuk memperoleh akses), dumpster diving (mengakses

untuk memperoleh password dan data lainnya), digital sniffing (pengamatan elektronik terhadap jaringan untuk mengungkap password atau data lainnya).

17. Sniffing
    Sniffing adalah penyadapan terhadap lalu lintas data pada suatu jaringan komputer.
18. Spoofing
    Spoofing adalah teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya "hal ini biasanya dilakukan oleh seorang hacker atau cracker".
19. Pharming
    Pharming adalah situs palsu di internet, merupakan suatu metode untuk mengarahkan komputer pengguna dari situs yang mereka percayai kepada sebuah situs yang mirip. Pengguna sendiri secara sederhana tidak mengetahui kalau dia sudah berada dalam perangkap, karena alamat situsnya masih sama dengan yang sebenarnya.
20. Malware
    Malware adalah program komputer yang mencari kelemahan dari suatu software. Umumnya malware diciptakan untuk membobol atau merusak suatu software atau operating system. Malware terdiri dari berbagai macam, yaitu: virus, worm, trojan horse, adware, browser hijacker, dll.

4. Hasil Pembahasan

4.1. Faktor Penyebab

Beberapa faktor yang menyebabkan kejahatan komputer (Cybercrime) adalah:

1. Akses internet yang tidak terbatas. Saling terhubungnyaantara jaringanyang satu dengan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya.
2. Kelalaian pengguna komputer.
3. Mudah dilakukan dengan resiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sangat sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatan untuk terus melakukan hal ini.
4. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu besar, dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh diatas operator komputer.
5. Kurangnya perhatian masyarakat dan penegak hukum..
6. Sistem keamanan jaringan yang lemah.
7. Cybercrime dipandang sebagai produk ekonomi.

4.2. Perkembangan Cybercrime Di Indonesia

Indonesia sebenarnya memiliki prestasi dalam bidang cybercrime ini. Walau di dunia nyata Indonesia dianggap sebagai salah satu negara terbelakang, namun prestasi yang sangat gemilang telah berhasil ditorehkan oleh para hacker, cracker dan carder lokal.

Virus komputer yang dulunya banyak diproduksi di US dan Eropa sepertinya juga mengalami "outsourcing" dan globalisasi. Di tahun 1986 – 2003, epicenter virus computer dideteksi kebanyakan berasal dari Eropa dan Amerika dan beberapa negara lainnya seperti Jepang, Australia, dan India. Namun hasil penelitian mengatakan di beberapa tahun mendatang Mexico, India dan Africa yang akan menjadi epicenter virus terbesar di dunia, dan Indonesia juga termasuk dalam 10 besar. Sehingga tidak akan lama lagi Indonesia akan terkenal namun dengan nama yang kurang bagus karena pemerintah kurang ketat dalam pengontrolan dalam dunia cyber.

Perkembangan cybercrime di Indonesia adalah kasus pornografi. Kegiatan yang termasuk pronografi adalah kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas.

Selain itu, kegiatan – kegiatan yang berpotensi cyber crime adalah sebagai berikut:

4.3. Contoh Kasus Cybercrime

1. Pada tahun 2008, Di Indonesia kasus pornografi yang terheboh baru-baru ini adalah kasusnya Ariel-Luna-Cut Tari. Kasus kejahatan ini memiliki modus untuk membuKasus ini terjadi saat ini dan sedang dibicarakan banyak orang, kasus video porno Ariel "PeterPan" dengan Luna Maya dan Cut Tari, video tersebut di unggah di internet oleh seorang yang berinisial 'RJ' dan sekarang kasus ini sedang dalam proses. Pada kasus tersebut, modus sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Penyelesaian kasus ini pun dengan jalur hukum, penunggah dan orang yang terkait dalam video tersebut pun turut diseret pasal-pasal sebagai berikut, Pasal 29 UURI No. 44 th 2008 tentang Pornografi Pasal 56, dengan hukuman minimal 6 bulan sampai 12 tahun. Atau dengan denda minimal Rp 250 juta hingga Rp 6 milyar. Dan atau Pasal 282 ayat 1 KUHP.
2. Prita Mulyasari, Digugat dan dilaporkan ke Polisi oleh Rumah Sakit Omni Internasional atas tuduhan Pencemaran nama baik lewat millis. Kasus ini bermula dari surat elektronik yang dibuat oleh Prita yang berisi pengalamannya saat dirawat di unit gawat darurat Omni Internasional. Prita Mulyasari dikenakan Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp.1 miliar
3. Narliswandi Piliang, wartawan yang kerap menulis disitus Presstalk.com , 14 Juli 2008 lalu di laporkan oleh Anggota DPR Alvin Lie ke Polda Metro Jaya. Kasus Tersebut bermula

dari tulisan Narliswandi Piliang yang berjudul "Hoyak Tabuik Adaro dan Soekanto", yang berisikan PAN meminta uang sebesar Rp 2 Triliun kepada Adaro agar DPR tidak lakukan hak angket yang akan menghambat IPO Adaro. Narliswandi Piliang dikenakan Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp. 1 miliar

4. Agus Hamonangan, adalah moderator milis FPK. Diperiksa sebagai saksi perkara pencemaran nama baik di Markas Kepolisian Daerah Metro Jaya. Pelapor kasus tersebut adalah Anggota DPR Fraksi Partai Amanat Nasional, Alvin Lie, terkait pemuatan tulisan berjudul "Hoyak Tabuik Adaro dan Soekanto", karya Narliswandi Piliang. Agus Hamonangan dikenakan pasal Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp 1 miliar
5. EJA (38) inisial, atas dugaan pencemaran nama baik dan penyebaran berita bohong melalui sistem elektronik. EJA dijadikan sebagai tersangka karena mengirimkan e-mail kepada kliennya soal lima bank yang dilanda kesulitan likuiditas, EJA telah resmi ditahan. Informasi EJA itu katanya dikhawatirkan akan menyebabkan rush atau kekacauan. Dikatakan bahwa EJA mendengar rumor soal sejumlah bank kesulitan likuidasi dari para broker secara verbal. EJA lalu menginformasikan hal itu kepada para kliennya melalui e-mail dengan domain perusahaannya. Informasi inilah yang lalu tersebar luas. EJA dikenakan Pasal 27 UU ITE ancaman hukuman 6 tahun penjara dan denda Rp. 1 miliar
6. Julian Assange, adalah seorang jurnalis yang berasal dari Australia yang dikenal sebagai pendiri dan juru bicara WikiLeaks. Hal ini dilakukannya karena dia yakin bahwa pertukaran informasi akan mengakhiri pemerintahan yang tidak sah. WikiLeaks memiliki server utama di Swedia. Julian Assange menyusup ke dalam sistem keamanan dan mempublikasikannya. Polisi Internasional bekerja sama untuk menangkap Julian Assange untuk mempertanggunjawabkan perbuatannya atas kebocoran informasi rahasia milik negara.
7. Edward Joseph Snowden, adalah mantan kontraktor teknik Amerika Serikat dan karyawan Central Intelligence Agency (CIA) yang menjadi kontraktor untuk National Security Agency (NSA) sebelum membocorkan informasi program mata – mata rahasia NSA kepada pers. Snowden membocorkan informasi rahasia menyangkut program – program NSA yang sangat rahasia seperti PRISM kepada The Guardian dan The Washington Post. Skandal Snowden membuat hubungan Amerika dan negara di Eropa seperti Prancis dan Jerman menjadi terganggu. Dari skandal Snowden ini juga akhirnya terkuak bahwa Australia selama ini menyadap telepon Presiden Indonesia, Susilo Bambang Yudhoyono serta beberapa jajaran staffnya yang membuat hubungan diplomatik Indonesia dan Australia menjadi terganggu. Saat ini Edward Snowden berada dalam perlindungan negara Rusia.

4.4. Penanggulangan Cybercrime

Untuk menanggulangi kejahatan internet yang semakin meluas maka diperlukan suatu kesadaran dari masing-masing negara akan bahaya penyalahgunaan internet. maka berikut adalah langkah ataupun cara penanggulangan secara global :

1. Modernisasi hukum pidana nasional berserta hukum acaranya diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
2. Peningkatan standar pengamanan system jaringan computer nasional sesuai dengan standar internasional.
3. Meningkatkan pemahaman serta keahlian aparat hukum mengenai upaya pencegahan, inventigasi, dan penuntutan perkara-perkara yang berhubungan dengan cyber crime.
4. Meningkatkan kesadaran warga Negara mengenai bahaya cyber crime dan pentingnya pencegahan kejahatan tersebut.
5. Meningkatkan kerja sama antar Negara dibidang teknologi mengenai hukum pelanggaran cyber crime.

Jadi, secara garis besar untuk penanggulangan secara global diperlukan kerja sama antara negara dan penerapan standarisasi undang-undang Internasional untuk penanggulangan Cyber crime.

4.5. Aspek Dan Penegakan Hukum Cybercrime

Aspek hukum yang istilahnya berasal dari Cyberspace Law, yang ruang lingkupnya meliputi ,setiap aspek yang berhubungan dengan orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai online dan memasuki cyber space atau dunia maya.

Menurut Jonathan Rosenoer dalam Cyber Law – The Law Of Internet menyebutkan ruang lingkup cyber law:

1. Copy Right
2. Trademark
3. Defamation
4. Hate Speech
5. Hacking, Viruses, Illegal Access
6. Regulation Internet Resource
7. Privacy
8. Duty Care
9. Criminal Liability
10. Procedural Issuses (Jurisdiction, Investigation, Evidence, etc)
11. Electronic Contract
12. Pornography
13. Robbery
14. Consumer Protection
15. E - Commerce, E - Government
16. Urgensi pengaturan cyber law di Indonesia adalah:
17. Kepastian hukum

18. Untuk mengantisipasi implikasi – implikasi yang timbul akibat pemanfaatan teknologi informasi
19. Adanya variable global, yaitu persaingan bebas dan pasar terbuka

Ruang lingkup Cyber Law di Indonesia adalah :

1. Hukum Publik : Juridiksi, Etika Kegiatan Online, Perlindungan Konsumen, Anti Monopoli, Persaingan Sehat, Perpajakan , Regulatory Body, Data Protection dan Cyber Crimes.
2. Hukum Privat : HAKI, E – Commerce, Cyber Contract, Domain Name, Insurance.

Penegakan hukum tentang cyber crime terutama di Indonesia sangatlah dipengaruhi oleh lima factor yaitu Undang-undang, mentalitas aparat penegak hukum, perilaku masyarakat, sarana dan kultur. Hukum tidak bisa tegak dengan sendirinya selalu melibatkan manusia didalamnya dan juga melibatkan tingkah laku manusia didalamnya. Hukum juga tidak bisa tegak dengan sendirinya tanpa adanya penegak hukum. Penegak hukum tidak hanya dituntut untuk professional dan pintar dalam menerapkan norma hukum tapi juga berhadapan dengan seseorang bahkan kelompok masyarakat yang diduga melakukan kejahatan.

Dengan seiringnya perkembangan jaman dan perkembangan dunia kejahatan,khususnya perkembangan cyber crime yang semakin mengkhawatirkan, penegak hukum dituntut untuk bekerja keras karena penegak hukum menjadi subjek utama yang berperang melawan cyber crime. Misalnya Resolusi PBB No.5 tahun1963 tentang upaya untuk memerangi kejahatan penyalah gunaan Teknologi Informasi pada tanggal 4 Desember 2001, memberikan indikasi bahwasanya ada masalah internasional yang sangat serius, gawat dan harus segera ditangani. Kitab Undang-undang Hukum Pidana (KUHP) masih dijadikan sebagai dasar hukum untuk menjaring cyber crime, khususnya jenis cyber crime yang memenuhi unsure-unsur dalam pasal-pasal KUHP. Beberapa dasar hukum dalam KUHP yang digunakan oleh aparat penegak hukum antara lain:

1. Pasal 167 KUHP
2. Pasal 406 ayat (1) KUHP
3. Pasal 282 KUHP
4. Pasal 378 KUHP
5. Pasal 112 KUHP
6. Pasal 362 KUHP
7. Pasal 372 KUHP

Selain KUHP adapula UU yang berkaitan dengan hal ini, yaitu UU No 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dimana aturan tindak pidana yang terjadi didalamnya terbukti mengancam para pengguna internet. Sejak ditetapkannya UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada 21 April 2008, telah menimbulkan banyak korban. Berdasarkan pemantauan yang telah aliansi lakukan paling tidak telah ada 4 orang yang dipanggil polisi dan menjadi tersangka karena diduga melakukan tindak pidana yang diatur dalam UU ITE. Para tersangka atau korban UU ITE tersebut merupakan pengguna internet aktif yang dituduh telah melakukan penghinaan atau terkait dengan muatan penghinaan di internet.

Orang-orang yang dituduh berdasarkan UU ITE tersebut kemungkinan seluruhnya akan terkena pasal 27 ayat (3) jo Pasal 45 ayat (1) UU ITE yakni dengan ancaman 6 tahun penjara dan denda 1 miliar rupiah. UU ITE dapat digunakan untuk menghajar seluruh aktivitas di internet tanpa terkecuali jurnalis atau bukan. Karena rumusannya yang sangat lentur.

Tindak pidana yang harus menjadi perhatian serius dalam UU ITE :

1. Pasal 27 (1)
   Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
2. Pasal 27 (3)
   Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan / atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
3. Pasal 28 (2)
   Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Aliansi menghimbau kepada pemerintah agar menarik kembali pasal-pasal tersebut dan merumuskan ulang sehingga dapat menjamin kebebasan menyatakan pendapat dan ekpresi para pengguna internet. Memasang kembali rambu-rambu yang lebih jelas mengenai larangan muatan internet. Aliansi juga meminta para pihak pengguna internet untuk tetap agar mendorong pemerintah dan Menteri Komunikasi dan Informatika untuk segera merevisi aturan ini karena pengguna internet merupakan calon korban terbesar dalam kasus-kasus tersebut. Secara khusus Aliansi meminta kepada pihak kepolisian agar tidak menggunakan intrumen cacat ini untuk kepentingan - kepentingan tertentu., seperti contoh kasus Prita Mulyasari, Narliswandi Piliang dll.

5. Kesimpulan

Berdasarkan data yang telah dibahas dalam makalah ini, maka dapat kami simpulkan, Cybercrime merupakan kejahatan yang timbul dari dampak negatif perkembangan aplikasi internet. Sarana yang dipakai tidak hanya komputer melainkan juga teknologi, sehingga yang melakukan kejahatan ini perlu proses belajar, motif melakukan kejahatan ini disamping karena uang juga iseng. Kejahatan ini juga bisa timbul dikarenakan ketidakmampuan hukum termasuk aparat dalam menjangkaunya. Kejahatan ini bersifat maya dimana si pelaku tidak

tampak secara fisik. Begitu hebatnya kejahatan ini bahkan dapat meresahkan dunia internasional. Dinamika cybercrime memang cukup rumit. Sebab, tidak mengenal batas negara dan wilayah.

Dari contoh kasus yg telah dipaparkan, maka dapat mengambil kesimpulan bahwa perkembangan teknologi yg sangat pesat terutama saat ini merupakan salah satu faktor kuat mengapa cybercrime saat ini sering terjadi. Meski sudah ada beberapa undang - undang tentang ITE, tapi dalam pelaksanaannya undang – undang tersebut masih sulit di jalani.

Perbaikan hukum atau membuat regulasi baru yg sesuai dgn masyarakat adalah salah satu jawaban atas maraknya cybercrime di indonesia. Namun bagian yang sangat penting adalah kesadaran masyarakat yang harus ditingkatkan. Sebaik apapun hukum yang diterapkan untuk mengatasi cybercrime, namun apabila masyarakat tidak mampu hidup mengikuti perkembangan teknologi informasi pada saat ini, maka hukum akan sia - sia.

DAFTAR PUSTAKA

Agus Raharjo SH.,M.Hum.Cybercrime (Pemahaman Dan Upaya Pencegaha Kejahatan Berteknologi).PT.Citra Aditya Bakti.Yogyakarta.2002

Hamzah , Dr.Andi. S.H.Aspek Aspek Pidana Di Bidang Komputer.Sinar Grafika.Cetakan Ke II.Jakarta.1987

Makarim, Edmon, S.Kom., S.H., LL.M. Pengantar Hukum Telematika. PT.Rajagrafindo Persada. 2005. Jakarta.

Makarim, Edmon, S.Kom., S.H., LL.M. Kompilasi Hukum Telematika. PT.Rajagrafindo Persada. 2003. Jakarta.

Sunarso Dr.Siswanto, SH,MH,MKn. Hukum Informasi Dan Transaksi Elektronik. PT Rineka Cipta. 2009.Jakarta

Muljono, Dr.Wahyu, SH K.n.Pengantar Teori Kriminologi.PustakaYustisia.Yogyakarta.2012

Sahetapy, J.E. Pisau Analisis Kriminologi.PT Citra Aditya Bakti.Bandung. 2005

Departemen Komunikasi dan informasi. Direktorat Jenderal Aplikasi Telematika.Buku Panduan Mengelola Warnet.Jakarta.2005

ND, Mukti Fajar & Achmad Yulianto, MH. Dualisme penelitian Hukum Normatif Dan Empiris.Pustaka Pelajar (Cetakan II). Yogyakarta. 2013