BAB I

PENDAHULUAN

A. Latar Belakang

Negara Indonesia adalah suatu organisasi yang benar, mempunyai tugas untuk pelaksanaan usaha pencapaian tujuan secara nasional dalam rangka mempertahankan meningkatkan kelestarian kehidupan bangsa dan Negara. Menjaga dan memelihara eksistensi Negara agar tetap bertahan hidup *(survive)*, bukanlah suatu hal yang mudah.

Dalam melaksanakan tugas Negara teknologi informasi sangatlah berperan penting, baik dimasa kini maupun dimasa yang akan dating. Teknologi informasi diyakini membaa keuntungan dan kepentingan yang besar lagi Negara-Negara di dunia. Setidaknya ada dua hal yang membuat teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia. Pertama, teknologi informasi mendorong permintaan atas produk-produk teknologi informasi intu sendiri, seperti komputer, modem, sarana untuk membagun jaringan internet dan sebagainya. Kedua, adalah memudahkan transaksi bisnis terutama keuangan disamping bisnis-bisnis umum lainnya.

Perpaudan teknologi komunikasi dan komputer melahirkan internet yang menjadi tulang punggung teknologi informasi. Perkembangan internet dipicu oleh peluncuran pesawat stupnik milik

uni soviet yang ditanggapi oleh Amerika Serikat dengan membuat peluncuran pesawat luar angkasa dan pengembangan internet pada tahun 1960-an pada awal perkembangannya, internet digunakan atau mengabdi kepada keepentingan khususnya kepentingan militer Amerika Serikat.

Perkembangan teknologi internet pada khususnya tidak dinikmati oleh orang-orang biasa seperti sekarang ini tetapi bermain dalam tingkat elit. Pengabdian total dunia teknologi terhadap kekuasaan Negara adalah inovasi perangkat perang sehingga muncul dari setiap akumulasi kekuasaan kaum bermodal melalui Negara adalah perang. Penaklukan antara Negara bukan sekedar memperluas wilayah untuk kepentingan kaum feudal, melainkan penguasaan sumber-sumber bagi mesin industri.

Kolonialisme berkembang dari rahim kapitalisme yang mengabaikan kemanusiaan. Sesuai perang dingin, internet tidak lagi digunakan untuk kepentingan militer, tetapu beralih fungsi menjadi sebuah media yang mampu membawa perubahan dalam kehidupan manusia. Internet tidak lagi hanya digunakan oleh kalangan militer, pemerintahan dan ilmuan, tetapi juga digunakan oleh pelaku bisnis, pilitikus, sastrawab, budayawan, musikus, bahkan para penjahat dan teroris. Internet mulai digunakan sebagai alat propaganda politik, transaksi bisnis atau perdangangan, sarana pendidikan, kesahatan,

manufaktur, perancangan pemerintahan, pornografi, dan kejahatan lain.

Perkembangan pesat dari teknologi telekomunikasi dan teknologi komputer menghasilkan internet yang multifungsi perkembangan ini membawa kita ke ambang revolusi keempat dalam sejarah pemikiran manusia, bila ditinjau dari konstruksi pengetahuan umat manusia yang dicirikan dengan cara berfikir tanpa batas *(boderkess way of thinking).* Percepaan teknologi semakin lama semakin supra yang menjadi sebab material perubahan yang terus menerus dalam semua interaksi dan aktivitas informasi.

Informasi yang didapat secara cepat, tepat dan akurat memainkan peranan sangat penting dalam berbagai aspek kehidupan manusia, seperti penentuan sebuah kebijaksanaan, sebagai trend atau gaya hidup manusia modern. Saat ini pemanfaatan teknologi menjadi suatu keharusan, tuntutan zaman dalam berbagai aspek tidaklah terlepas dari peran penting teknologi. Kalangan bisnis, organisasi, perkantoran, pendidikan, dan militer hingga individu yang menjadu sangat ketergantungan dengan fenomena zaman informasi. Sehingga muncullah istilah yang sering dikenal dengan sebutan *"the information age"* atau abad informasi.

Kemudahan dan kenikmatan yang ditawarkan abad informasi tidak hanya membawa dampak positif, tapi juga sekaligus membawa ancaman bagi masyarakat dan Negara. Hal ini ditandai dengan

munculnya berbagai kasus *cyber* yang mengancam keamanan para pengguna internet di Indonesia. Kejahatan besar dengan bahan bakan teknologi di abad ke-21.

Perkembangan *cyber crime* sering dibahas di berbagai forum internasional. Kongres PBB mengenai *The Prevention of Crime and the Treatment of offenders,* (yang sejak Konres XI/2005 berubah menjadi *congress on crime prevention and criminal justice)* telah membahas masalah ini sampai tiga kali, yaitu pada Kongres VIII/1990 di Havana.

Kongres X/2000 di Wine, dan terakhir pada Kongres XI/2005 di Bangkok (tanggal 18-25 April. Disamping itu, telah ada pula Konvensi *cyber crime* Dewan Eropa *(council of Europe cyber crime convention)* yang ditandatangani di Budapest pada tanggal 23 November 2001 oleh berbagai Negara, termasuk Kanada, Jepang, Amerika, dan Afrika selatan. Sebagaimana yang ditaungkan dalam *convention on cybercrime.* mengamanatkan bahwa :

Pihak Negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana antara lain, secara serius merintangi fungsi dai sebuah sistem komputer dengan tanpa hak melalui memasukkan, memindahkan merusak, menghapus, memperbaiki, memperburuk, mengubah dan menahan data komputer.

Setiap pihak Negara harus menerapkan undang-undang dan menerapkan tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana antara lain, melakukan secara sengaja dan tanpa hak, memasukkan, mengubah, menghapus, atau menahan data komputer, menyebabkan data menjadi tidak seperti aslinya dengan maksud bahwa hal itu dianggap atau dilakukan untuk sebuah tujuan hukum tertentu seakan akan asli, tanpa mempertimbangkan apakah data tersebut bida dibaca dan bisa dimengerti secara langsung. Pihak Negara dapat mensyaratkan maksud untuk menipu atau maksud tidak jujur lainnya sebelum konsekuensi mengikat.

Selain itu terdapat juga *international convention for the suppression of terroris bombing* yang mengamanatkan bahwa:

Setiap Negara pihak wajib mengambil tindakan-tindakan yang diperlukan, termasuk, bila sesuai, peraturan dalam negeri, untuk memastikan bahwa tindak pidana dalam ruang lingkup konvensi ini, khususnya dimana mereka dimaksudkan atau dihitung memprovokasi keadaan terror di masyarakat umum atau dalam kelompok orang atau orang-orang tertentu, berada di bawah dibenarkan dengan pertimbangan yang sifatnya serupa politik, filsafat, ideology, ras, etnis, agama atau lainnya dan dijatuhi hukuman yang sesuai dengan alam kubur mereka

Indonesia telah memiliki *cyber law* yang diatur dalam undang-undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. Saat ini juga telah disusun draft *International Convention To Enhance Protection From Cyber Crime and Terrorism* yang membahas tentang peningkatan perlindungan dari kejahatan *cyber* yang merupakan kejahatan terorisme.

Berikut ini adalah beberapa contoh kasus *cyber crime* yang pernah terjadi di Indonesia.

Pertama adalah kejahatan kartu kredit, POLDA daerah istimewah Yogyakarta telah menangkap lima carder dan mengamankan barang bukti bernilai puluhan juta, yang didapat dari merchant luar negeri. Begitu juga dengan yang dilakukan mahasiswa sebuah perguruan tinggi di Bandung. Akibat perbuatannya selama setahun, beberapa pihak di jerman dirugikan sebesar 15.000 DM (sekitar Rp 70 juta) para carder beberapa waktu lalu juga menyadap data kartu kredit dari dua outlet pusat perbelanjaan yang cukup terkenal.

Caranya, saat kasir mengesek kartu pada waktu pembayaran. Pada saat data berjalan ke bank-bank tertentu itulah data dicuri. Akibatnya, banyak laporan pemegang kartu kredit yang mendapatkan tagihan terhadap transaksi yang tidak pernah dilakukannya. Modus kejahatan ini adalah penyalahgunaan kartu kredit oleh orang lain yang tidak berhak. Motif kegiatan dari kasus ini termasuk ke dalam *cyber crime* sebagai tindakan murni kejahatan.

Hal ini dikarenakan si penyerang dengan sengaja menggunakan kartu kredit milik orang lain.

Kasus *cyber crime* ini merupakan jenis carding. Sasaran dari kasus ini termasuk kedalam jenis *cyber crime* menyerang hak milik *(against property)* sasaran dari kasus kejahatan ini adalah *cyber crime* menyerang pribadi *(against person).*

Kedua, penyerang terhadap jaringan internet Komisi Pemilihan Umum (KPU). Jaringan di internet di Pusat Tabulasi Nasional Komisi Pemilihan Umum sempat *down* (terganggu) beberapa kali, KPU menggandeng kepolisian untuk mengatasi hal tersebut. Kasus ini memiliki modus untuk mengacaukan proses pemilihan suara di KPU. Motif kejahatan ini termasuk ke dalam *cyber crime* sebagai tindakan murni kejahatan. Hal ini dikarenakan para penyerang dengan sengaja untuk melakukan kekacauan pada tampilan halaman tabulasi national hasil dari Pemilu.

Kejahatan kasus *cyber crime* ini dapat termasuk jenis data *forget, hacking-cracking, abotage and extortion,* atau *cyber terrorism*. Sasaran dari kasus ini adalah *cyber crime* menyerang pemerintah *(againt govermment)* atau bias juga *cyber crime* menyerang hak milik.

Ketiga, puluhan situs milik Indonesia berhasil disusupi hacker yang mengaku berasal dari Malaysia. Situs-situs asal Indonesia itu berhasil di *defance* dengan menyertakan gambar alien dan dua buah blog yang masing-masing dimiliki warna Negara Malaysia dan warga Negara Indonesia. Saat ditelusuri, Senin (24/11/2008), rupanya telah terjadi perseteruan antara *Hacker* asal Malaysia. Korban serangan

tersebut diantaranya situs pemuda hanura, gerbang linux, KBRI Beirut, FK usakti 95, dan masih banyak lagi. Beberapa situs Malaysia pun mengalami aksi serupa akibat *defance* balasan dari *hacker* Indonesia justru mengambil tema ganyang meligsial. Jika terus berkelanjutan, hal ini akan memicu adanya perang *cyber* di dunia maya.

Beberapa kasus diatas menjadi suatu pelajaran dan peringatan penting bagi aparat penek hokum serta seluruh anggota internet untuk memberikan perhatian khusus akan ancaman yang terus mengintai di dunia di dunia maya.

Beberapa kasus diatas menjadi suatu pelajaran dan peringatan penting bagi aparat penek hokum serta seluruh anggota internet untuk memberikan perhatian khusus akan ancaman yang terus mengintai di dunia *cyber space*. Peluang kejahatan ini juga mengundang para terorisme di dunia maya *(cyber terrorism)* untuk turut serta berpetuaalang didalamnya *cyber terrorism,* sebuah kata yang masih asing bagi khalayak umum. Sebagai suatu bentuk kejahatan, *cyber terrorism* merupakan bentuk perkembangan dari *cyber crime. Cyber crime* sendiri merupakan salah satu bentuk atau dimensi baru dari kejahatan masa kini yang mendapat perhatian luas dari dunia internasional.

Dalam beberapa kasus, penguasaan terhadap teknologi sering kali disalah gunakan untuk melakukan suatu kejahatan. Diantara

raga kejahatan menggunakan teknologi, terdapat didalamnya suatu bentuk kejahatan terorisme baru, yaitu *cyber terrorism.* Akar perkembangan dari *cyber terrorism* dapat ditelusuri sejak awal 1990, ketika pertumbuhan internet semakin pesat dan kemunculan komunitas informasi.

Di Amerika Serikat sejak saat itu diadakan kajian mengenai potensi resiko yang akan dihadapi Amerika Serikat atas ketergantungannya yang begitu erat dengan jaringan *(networks)* dan teknologi tinggi. Dikawatirkan, karena ketergantungan Amerika Serikat yang begitu tinggi terhadapt jaringan dan teknologi suatu saat nanti Amerika akan menghadapi apa yang disebut *"Electronic pearl Harbor".*

Factor psikologis, politik, dan ekonomi merupakan kombinasi yang menjadikan peningkatan ketakutan Amerika terhadap isu terkait *cyber terrorism*. Sehingga pada tahun 1999, Presiden Clinton sampai mengajukan proposal anggaran dana untuk menangani aksi *cyber terrorism* sebesarsarsar $ 2,8 miliar. Dana tersebut juga diperuntukan bagi penanganan keamanan nasional dari ancaman bahaya internet. Ketakutan tersebut cukup beralasan, karena telah terjadi beberapa insiden yang dikategorikan sebagai *cyber terrorism,* antara lain pada april dan maret 2002, di Amerika Serikat, tepatnya Negara California, terjadi kehilangan pasokan listrik secara total yang disebabkan oleh ulah *cracker* dari Cina yang menyusup

kedalam jaringan *power generator* di wilayah tersebut. Contoh lain adalah *Hacking* pada system penerbangan sipil komersial yang mengacaukan system komputer bandara Nagoya yang hampir merenggut korban nyawa.

Menurut penulis ancaman *cyber crime* akan terus mengalami perkembangan yang sangat pesat, seiring dengan perkembangan dan kemajuan dunia teknologi informasi. Masyarakat Indonesia da aparat penek hokum harus lebih siap dalam menghadapi ancaman *cyber crime.* Begitu pula dengan pengaturan dan bela hokum penanggulangan kejahatannya harus tetap diperhatikan. Pada awalnya hokum Indonesia tidak mampu mengantisipasi munculnya kejahatab di dunia *cyber space*, dan pada akhirnya lahirlah Undnga-Undang No.11 tahun 2008 tentang informasi dan transaksi elekronik yang dianggap mampu memberi solusi namun masih saja manual kontroversi.

Berdassarkan fakta diatas dan kompleksnya permasalahan *cyber crime* dalam eskalasi nasional dan internasional, maka penulis tertarik untuk mengkasi persoalan kejahatan *cyber crime* ditinjau dari perspektif kriminologi kontemporer.

B. Rumusan Masalah

1. Bagaimanakah *Cyber Crime* ditinjau dari perspektif kriminologi kontemporer?

2. Bagaimanakah pemberlakuan hukum pidana ini terhadap *cyber crime* ?

C. Tujuan Penelitian

1. Menjelaskan bagaimana *cyber crime* ditinjau dari perspektif kriminologi kontemporer.
2. Mejelasskan bagaimana pemberlakuan hukum pidana saat ini terhadap *cyber crime.*

D. Kegunaan Penelitian

1. Kegunaan teoritis, memberikan sumbangan akademik untuk menambah variasi kajian dan pemahaman teoritis mengenai *cyber crime* ditinjau dari perspektif kriminologi kontemporer.
2. Kegunaan praktis, memberikan masukan berguna baik kepada kalangan akademisi, aparat penegak hokum, lembaga swadaya masyarakat, serta masyarakat umum, terkait dengan *cyber crime* ditinjau dari perspektif kriminologi kontemporer.