ANTI CYBER TERORISM SEBAGAI UPAYA STRATEGIS DALAM MENANGGULANGI *VYBER TERORISM* DI INDONESIA

Gilang Muhammad Mumtaaz, Thariq Rafif Wardhana, Fibiya Harnung Diastutui

Fakultas Hukum, Universitas Diponegoro

gilangmuhtaz@gmail.com

ABSTRAK

Karya Tulis Ilmiah ini berupaya menjelaskan secara ringkas berkaitan dengan seperangkat isu-isu yang berkaitan dengan cyberterrorism. Selain itu juga ke depan perlu dipikirkan tentang kebijakan antisipatif hukum pidana dalam mengeliminir terjadinya cyberterrorism sebagai trend of crime. Analisa menunjukan bahwa cyberterrorism merupakan bentuktransformasi terror yang dilakukan oleh teroris dengan menjadikanjaringan internet sebagai alat atau sasaran serangan. Jenis kejahatan ini bermetamorfosis menjadi kejahatan yang bersifat lintas negara. Pelakunya bisa berasal dari wilayah negara mana saja yang berakibat hukum pada identitas yang berimplikasi pada penentuan yurisdiksi pengadilan. Dengan pola yang cukup maju ini maka dibutuhkan kerjasama yang bersifat global atau inter negara. Salah satusolusinya setiap negara harus melakukan sinkronisasi tentang peraturan perundang- undangan yang khusus mengatur tentang cyberterror.

Kata Kunci: Kebijakan Pidana, *Cyberterrorism*, Negara.

ABSTRACT

This scientific paper attempts to explain briefly related to a set of issues relatedto cyberterrorism. In addition, in the future, it is necessary to think about anticipatory policies of criminal law in eliminating the occurrence of cyberterrorism as a trend of crime The analysis shows that cyberterrorism is a form of terror transformation carried out by terrorists by making the internet network as a toolor target of attack. This type of crime metamorphosed into a crime that was transnational in nature. The perpetrators can come from the territory of any country which has a legal effect on identity which has implications for determining the jurisdiction of the courts. With this fairly advanced pattern, global or international cooperation is needed. One solution is that each country must synchronize the laws and regulations that specifically regulate cyberterror.

Keywords: Criminal Policy, Cyberterrorism, State.

A. Pendahuluan

Sejalan dengan Pembukaan Undang-Undang Dasar 1945, maka negara republik Indonesia adalah negara kesatuan yang berlandaskan hukum dan memiliki tugas dan tanggung jawab untuk memelihara kehidupan yang damai serta secara aktif turut serta dalam mememelihara perdamaian dunia.[1] Salah satu permasalahan yang marak dibicarakan baik melalui media cetak maupun media elektronik adalah isu terkait terorisme. Jika menilik sejarahnya, terorisme menjadi permasalahan yang sangat serius di Indonesia pasca adanya peristiwa serangan bom Bali pada November tahun 2002. Sudah barang tentu segala bentuk tindakan terorisme tidak dapat dibenarkan apapun motivasinya, kapanpun tempatnya dan siapapun yang menjadi targetnya. Sebagai Negara yang mempunyai kewajiban dalam melindungi harkat dan martabat manusia, Indonesia telah menciptakan peraturan perundang undangan yang mengatur tentang terorisme dalam rangka melindungi warga Negara terhadap aksi terorisme. Upaya ini telah diwujudkan pemerintah dengan mengeluarkan Undang-Undang Republik Indonesia nomor 5 Tahun 2018 yang merupakan Perubahan Atas Undang Undang nomor 15 Tahun 2003 tentang penetapan Peraturan Pemerintah Pengganti Undang-Undang nomor 1 Tahun 2002 tentang tindak pidana terorisme. Peraturan Perundang- Undangan ini sangat diperlukan karena mengingat tindak pidana Terorisme merupakan suatu kejahatan luar biasa (*extra ordinary crime*) serta membutuhkan penanganan yang luar biasa pula (*extra ordinary measures*).[2]

Pasal 1 Undang-undang Nomor 5 tahun 2018 menyebutkan terorisme adalah perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana teror atau rasa takut secara meluas, yang dapat menimbulkan korban yang bersifat massal dan/atau menimbulkan kerusakan atau kehancuran terhadap objek vital yang strategis, lingkungan hidup, fasilitas publik, atau fasilitas internasional dengan motif ideologi, politik atau ganggaun keamanan. Terorisme secara kasar merupakan suatu istilah yang digunakan

[1] Susan W. Brenner, 2007, Cybercrime: Re-Thinking Crime Control Strategies, dalam Yvonne Jewkes (edt), Crime Online, USA: Willan Publishing, hlm. 13

[2] Joel P. Trachmant, 2006, Global Cyberterrorism, Jurisdiction, And International Joel P. Trachmant, 2006, Global Cyberterrorism, Jurisdiction, And International

untuk penggunaan kekerasan terhadap penduduk sipil atau non kombatan untuk mencapai tujuan politik dalam skala yang lebih kecil daripada perang. Darisegi bahasa, istilahteroris berasal dari Perancis pada abad ke delapan belas. Kata terorisme yang artinya dalam keadaan teror (under the terror) berasal dari bahasa latin "terrere" yang berarti gemetaran dan"detererre" yang berarti takut.[3]

Pengertian Terorisme untuk pertama kali dibahas dalam *EuropeasConvention on the Supression on Terrorism* (ECST) di Eropa pada tahun 1977 terjadi perluasan paradigma arti dari *Crimes against State* menjadi *Crime Against Humanity*. *Crimes Against Humanity* meliputi tindak Pidana untuk menciptakan suatu keadaan yang mengakibatkan individu, golongan dan masyarakat umum ada dalam suasana yang teror. Perkembangan teknologi juga mengakibatkan perkembangan di berbagai bidang dan menciptakan globalisasi yang berpengaruh kepada berbagai bidang seperti politik, sosial, perdagangan dan kriminalitas yaitu salah satunya terorisme.[4] Terorisme mempunyai pengaruh kuat terhadap masyarakat terutama jika dipublikasikan secara ekstrim oleh media cetak atau elektronik.

Dalam Pasal 1 Undang-Undang nomor 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisa, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkaninformasi elektronik Kehadiran internet terbentuk melalui jaringan komputer yang menghubungkan antar negara atau antar benua yang berbasis transmission control protocol/internet protocol. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda. Internet (*cyberspace*) sendiri bagai koin yangmemiliki dua sisi, disatu sisi internet dengan berbagai manfaatnya dapat membantu perkembangan suatu negara dan mempermudah menyebarkan informasi sehingga membuatmasyarakat dunia lebih *up to date*, namun disisi lain internet dapat dimanfaatkan oleh orang-orang yang ingin

[3] *Ibid.*
[4] Andrew Michael Colarik.2006, Cyber Terrorism: Political and Economic Implications, Idea Group: USA, hlm. 15

melakukan perilaku hukum yang menyimpang dengan memanfaatkanjaringan Internet dalam gerakan masif dalam menyebarkan Ideologi dari kelompok radikalyang menginginkan pihak lain percaya bahwa tindakan yang dilakukannya adalah hal yang benar.[5] Selanjutnya melakukan tindakan lebih lanjut dengan meyakinkan bahwa pemerintahan yang sedang berdaulat perlu dihancurkan dengan sebuah tindakan yang nyata di luar ruang lingkup *cyber* dengan menimbulkan ancaman dan menyebarkan rasa takut pada semua orang yang dikenal dengan teror. Jaringan internet ini dimanfaatkan oleh pelaku terorisme untuk menunjang kegiatan teroris mereka, penggunaan internet oleh teroris dikenal dengan "*terrorist use The Internet*". Lebih lanjut, penggunaan internet oleh teroris atau sekelompok orang untuk melakukan kejahatan terorisme dikenal dengan *cyber terrorism*. Dengan menggunakan jaringan internet, para teroris dapat dengan mudah melakukan serangan karena lewat jaringan internet mereka akan sulit untuk diidentifikasikan.[6]

Cyber terrorism atau terorisme dunia maya adalah bentuk kejahatan baru yang memiliki karakteristik dan bentuk tersendiri.[7] *Cyber terrorism* diidentifikasikan sebagai serangan terhadap infrastruktur nasional yang kritis atau intimidasi terhadap warga sipil dan pegawai pemerintahan dengan menggunakan jaringan dan tekhnologi komputer.[8] *Cyber terrorism* juga dianggap sebagai serangan yang melanggar hukum terhadap jaringan komputer, jaringan informasi yang tersimpan yang bertujuan untuk mengintimidasi pemerintah atau rakyatnya. Serangan tersebut menghasilkan kekerasan terhadap individu, kelompok atau properti pemerintah dan menimbulkan bahaya dan ketakutan. Sistem satelit, telekomunikasi, perbankan, pengendalian lintas udara, sistem navigasi laut, jaringan telekomunikasi, distribusi listrik, jaringan pertahanan dan keamanan termasuk sistem pengendalian *weapon of mass destruction* (WMD) terasuk bom nuklir, kesehatan dan bentuk-bentuk fasilitas pelayanan publik lainnya menjadi sasaran kejahatan kaum teroris.

---

[5] Barda Nawawi Arief, 2006, Tindak Pidana Mayantara Perkembangan Kajian Cybercrime, Indonesia, Jakarta : RajaGrafindo Persada, hlm. 21
[6] *Ibid.*
[7] Janet J. Prichard Laurie E. MacDonald, 2004, Cyber Terorism: A study of the extent coverage in computer security textbook, *Journal of Information technology education*, Volume 3. 200, hlm. 280
[8] *Ibid.*

Ancaman perbuatan *cyber terrorism* dapat menimpa semua Negara tak terkecuali Indonesia. Pemanfaatan sarana internet dalam melakukan kegiatan terorisme perlu diwaspadai karena hampir seluruh fasilitas Negara, fasilitas umum dan kegiatan masyarakat menggunakan jaringan internet yng mempunyai fleksibilitas yang dapat menghubungkan segalanya.

Serangan *cyber* dapat menimbulkan korban sama halnya dengan terorisme yang dilakukan dengan cara konvensional. Untuk sementara ini belum ada peraturan perundang-undangan yang mengatur secara jelas mengenai *cyber terrorism* di Indonesia sehingga menimbulkan keraguan apabila seandainya tindak pidana ini terjadi di Indonesia apakah harus memakai dasar hukum apa untuk menjerat tindak pidana ini, seperti dalam pasal 1 ayat (1) KUHP yang berbunyi ”Suatu perbuatan tidak dapat dipidana, kecuali berdasarkan ketentuan perundangundangan yang telah ada” yang juga dikenal dengan asas legalitas atau asas nullum delictum *nulla poena sine praevia liege poenali* (tidak ada delik, tidak ada pidana lebih dulu). Namun asas ini tidak berarti tidak memperbolehkan melakukan penafsiran terhadap rumusan delik yang ada dalam peraturan perundang undangan. Sehingga apabila terjadi tindak pidana *cyber terrorism* dapat dilakukan penafsiran terhadap peraturan perundang- undangan yang telah ada dan berhubungan terhadap tindak pidana ini, dalam hal ini yaitu Undang- Undang nomor 5 Tahun 2018 tentang Pemberantasan Terorisme dan Undang-Undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik.

B. Pembahasan

1.Problematika Cyber Terorism Sebagai Bentuk Kejahatan Internasional

Cyber Terorism bukan lagi suatu fenomena tetapi telah secara nyata menjadi suatu bentuk kejahatan. Dalam bab sebelumnya telah disebutkan bahwa *Cyber Terorism* merupakan konvergensi antara *cyberspace* dengan terorisme. Hal ini memberikan dampak negatif pada sistem komunikasi dan sistem infrastruktur yang telah menggunakan jaringan internet maupun satelit. Luasnya daya jangkau jaringan internet (borderless) memberikan keuntungan bagi para pelaku kejahatan terorisme atau kejahatan siber. Kejahatan yang dilakukan oleh mereka dapat mengancam keamanan nasional maupun internasional. Menilik dari bagaimana dampak *Cyber*

Terorism, dalam sub bab ini akan dijelaskan apakah *Cyber Terorism* merupakan bentuk kejahatan internasional atau tidak. Untuk menyebut *Cyber Terorism* sebagai kejahatan internasional perlu diperhatikan apakah unsur unsur *cyber terrorism* ini memenuhi unsur-unsur sebagai kejahatan internasional. Pada bagian ini penulis akan menjelaskan unsur-unsur *Cyber Terorism*, unsurunsur kejahatan internasional dan kejahatan transnasional.

Belum ada penggunaan komputer secara jahat yang memenuhi definisi *Cyber Terorism*, untuk menyebabkan kehancuran dengan sarana komputer adalah hal yang sangat sulit. Sehingga, ancaman *cyber terrorism* lebih dianggap masuk akal sebagai suplemen bagi serangan teroris yang lebih besar. Selain itu, untuk menyebut suatu serangan komputer sebagai *Cyber Terorism* merupakan hal yang problematik, karena sulit menentukan niat, identitas, atau motivasi politik dari penyerang secara pasti sampai kejadian tersebut telah berlangsung cukup lama. Suatu *cyber crime* berupa serangan pada sistem elektronik harus dibedakan dengan *Cyber Terorism*. Serangan disebut sebagai *cyberterrorism*, selain adanya penggunaan teknologi, harus dilihat pula identitas orang yang melakukannya, motif dan tujuan yang mereka lakukan, serta akibatnya. Serangan *cyber terrorism* haruslah berakibat pada kekerasan pada orang atau barang atau setidaknya cukup menyebabkan ancaman bahaya untuk menimbulkan ketakutan. Sebab, meskipun dilakukan dalam suatu sistem elektronik, serangan *Cyber Terorism* ini tetap terdiri dari unsur-unsur yang umumnya terdapat pada terorisme.

Terdapat dua bentuk kegiatan *Cyber Terorism*, yaitu bentuk *cyberterrorism* sebagai serangan dan sebagai pendukung. Dalam bentuk kegiatan *Cyber Terorism* sebagai serangan, teknologi informasi merupakan alat dan objek serangan. Suatu serangan *Cyber Terorism* untuk memenuhi unsur terorisme yang menimbulkan rasa takut yang meluas, adalah berupa serangan langsung pada sistem komputer yang berakibat ancaman terhadap nyawa, misalnya mengacaukan sistem kontrol pesawat atau mengacaukan rekaman medis suatu rumah sakit. Serangan tersebut juga ditunjukan pada infrastruktur penting yang digunakan untuk kehidupan orang banyak, sehingga gangguan terhadap infrastruktur tersebut dapat mengakibatkan dampak yang menimbulkan ancaman fisik maupun rasa takut meluas. Bentuk Cyber Terorism yang kedua adalah sebagai pendukung, dimana jaringan sistem informasi digunanakan teroris untuk keperluan organisasinya. *Cyber Terorism* sendiri belum diatur secara khusus dalam

suatu aturan atau undang-undang baik secara nasional maupun internasional. Dalam hal pemberian sanksi atau pemidanaan pada kegiatan cyberterrorism diatur dalam konvensi-konvensi atau undang undang yang berkaitan dengan *Cyber Terorism*. Dalam *Convention on Cybercrime*, pemidanaan atau pemberian sanksi terhadap pelaku kejahatan *cyber* diserahkan sepenuhnya kepada negara yang telah meratifikasi atau mengaksesi konvensi tersebut. Pidana yang dapat dijatuhkan kepada pelaku pelanggaran menurut konvensi ini adalah sanksi yang efektif, proporsional, dan dapat mendidik,termasuk pidana penjara. Hal ini diuraikan dalam Pasal 13 yang berbunyi sebagai berikut:

Article 13 – Sanctions and measures

(1) Each Party shall adopt such legislative and other measures as mas be necessary to ensure that the criminal offence establishedin accordance with Article 2-11 are punishable by effective, proportionate and dissuasive sanction, which include deprivation of liberty.

(2) Each Party shall ensure that legal person held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanction or measurea, including metary sanction.

2. Anti Cyber Terorism Sebagai Upaya Strategis dalam Menanggulangi Cyber Terorism di Indonesia

Cyberterrorism merupakan kejahatan yang cukup sulit untuk dikontrol dan diperangi karena muncul diantara beberapa sistem hukum. Dengan lokasi dan karakter *cyberterrorism* yang bersifat lintas nasional menjadi kesulitantersendiri yang berlanjut pada persoalan juridiksi. Persoalannya juga menjadi bertambah yaitu tiadanya kesepahaman hukum tentang jenis perbuatan apa saja digolongkan sebagaitindak pidana di antara berbagai sistem hukum yang ada sehingga menambah berbahayanyagambaran kejahatan ini. Oleh karena itu, pembahasan pada bagian ini mengeksplorasi tentangpendekatan teknologi sebagai salah satu model *control of cyberterrorism*. Selain pengarus-utamaan pendekatan tersebut sebagai kebijakan yang paling strategis maka pendekatan penal(*penal policy*) menjadi kebijakan yang bersifat komplementer/ pelengkap untuk menghadapi cyberterrorism.

Tentunya terlebih dahulu dengan melakukan sinkronisasi internal danpengaturan yang bersifat *inter state* atau global. Tujuannya agar kebijakan antisipatif hukumpidana menjadi respon terukur dan sistematis sebagai bagian kebijakan yang rasional untuk mengantisipasi *cyberterrorism*. Upaya menanggulagi *cyberterrorism* dengan:

1) Pendekatan Teknologi (*Techno Prevention*)

Hukum pidana tidak akan mampu bekerja sendiri. Berdasarkan penelitian ini maka cara yang harus diutamakan adalah menghilangkan faktor faktor pada level penyebab atau akar masalah. Seperti dijelaskan pada bagian awal penelitian ini, *cyberterrorism* adalah jenis kejahatan yang terkait erat dengan teroris yang menggunakan teknologi maju sebagai sarana atau sasaran serangan. Maka upaya yang paling rasional dalam menghadapi varian baru dari kejahatan tersebut adalah mengutamakan pendekatan teknologi (*techno prevention*). Model prevensi ini menjadi actual karena keterbatasan hukum pidana itu sendiri yang bersifat *post factum*. Maksudnya, respon hukum pidana lahir ketika kejahatan sudah terjadi. Model pendekatan ini tidak lagi strategis dan efektif untuk menjawab munculnya persoalan kejahatan yang relatif baru karena pengaruh langsung dari kemajuan teknologi. Untuk menjawab tuntutan itu maka ke depan perlu dipikirkan beberapa upaya alternatif untuk melakukan kontrol terhadap *cyberterrorism*. Salah satunya adalah pendekatan yang berbasis teknologi yaitu *Biometric Technology*. Salah satu persoalan yang menjadi masalah dalam kejahatan *cyberterrorism* adalah soal penentuan akan identitas seseorang. Identitas merupakan soal yang cukup kompleks dan multi wajah, maka cara terbaik untuk memahaminya harus dibagi dalam tiga kategori yaitu secara pribadi, sosial dan hukum. Untuk menyederhanakan pembahasan, penelitian ini, memfokuskan pada persoalan identitas hukum (*legal identity*). *Legal identity* yaitu terdiri dari penetapan kelahiran dengan pokok-pokok yang mencakup akta kelahiran, menjelaskan secara jelas keunikan sejarah tentangdata diri seseorang tentang nama yang diberikan, jenis kelamin, tanggal dan tempat kelahiran termasuk keterangan tentang siapa orang tuanya. Identitas hukum (*legal identity*) seringkali dalam dunia siber disamarkan, dipalsukan atau dicuri. Dengan menggunakan data diri yang disamarkan seorang teroris bisa mengakses jaringan, data untuk melancarkan aksinya. Untuk memecahkan persoalan

tentangpenyalahgunaan data diri seseorang untuk melakukan serangan teror maka cara antisipatif yang dapat digunakan yaitu mengaktifkan teknologi biometrics. Logika dasar yang dipakai teknologi ini adalah aplikasi teknologi untuk melakukan kontrol dan pembatasan atasakses internet. Sebagai contoh Biometric Jerman yang diatur dalam KUHP Jerman (*German systems* terdiri dari dua proses: yaitu pendaftaran (enrolment) dan penyesuaian (*matching*). Pada tahap pendaftaran, untuk pertama kali karateristik individu haruslah mencakup sidik jari. Gambar yang diperoleh pada umumnya dapat dirubah menjadi sebuah template. Pada fase penyesuaian (*matching*) biometrika yang menggambarkan karateristik individu tadi disesuaikan dengan *live template* dengan membandingkan data sebelumnya apakah sesuai atau tidak. Kata kunci untuk bekerjanya system biometrik didalam cara verifikasi.

2) Sinkronisasi Legislasi Penal (*Penal Approach*)

Salah satu sifat dari *cyberterrorism* adalah sifatnya yang melintasi batas negara. Persoalan kemudian hukum suatu negara harus berorientasi pada bagaimana melakukan upaya harmonisasi. Tujuannya agar sistem hukum suatu negara tidak mengalami tumpah tindih baik di internal negara bersangkutan (harmonisasi internal/ke dalam) atau harmonisasi dengan negara lain ataupu instrument hukum internasional (harmonisasi eksternal/ke luar)

3) Harmonisasi Eksternal

Persoalan *cyberterrorism* merupakan persoalan lintas negara. Pelaku, korban, sasaran, kerugian, yurisdiksi bisa berada jauh dari teritorial di mana hukum suatu negara berlaku. Oleh karena itu, harmonisasi substansi legislasi antar negara satu dengan negara lain menjadi penting. Tujuannya agar kepentingan hukum yang hendak dilindungi oleh norma hukum pidana menjadi kesepahaman inter negara atau interteritorial yang wajib dilindungi bersama. Sebagaimana tertulis di atas bahwa telah tersaji salah satu perspektif kebijakan legislasi dari negara luar seperti halnya Jerman. Komparasi ini menjadi penting sebagai bahan perbandingan dan masukan bagi hukum pidana Indonesia dalam menyikapi cyberterrorism.

4) Harmonisasi Internal

Memasuki persoalan harmonisasi internal dimana Indonesia setidaknya telah mengesahkan salah satu Rancangan Undang Undang yang berkaitan dengan kejahatan dunia maya (*cybercrime*) yaitu Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Undang-Undang ini bertujuan untuk mengharmonisasikan antara instrumen peraturan hukum nasional dengan instrumen-instrumen hukum internasional. Adapun lebih lanjut mengenai berbagai instrument hukum nasional yang mengatur teknologi informasi di antaranya, yaitu:

- **UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik**

UU No. 11 Tahun 2008 merupakan undang-undang yang mengatur tentang kejahatan-kejahatan yang berbasis teknologi(*cyber crime*), sedangkan tindak pidana CT merupakan bagian/jenis dari *cyber crime*. Ketentuan pidana dalam UU ITE terdapat dalam Bab XI Pasal 45 sampai dengan Pasal 52. Berikut perumusan beberapa pasal dalam Bab XI mengenai ketentuan pidana. Berdasarkan ketentuan pasal-pasal dalam Bab XI mengenai ketentuan pidana dalam UU ITE, maka dapatdiidentifikasikan beberapa perbuatan yang dilarang (unsur tindak pidana) yang erat kaitannya dengan tindak pidana CT pada tiap tiap pasalnya. Pasal 30 Terkait dengan aksi kejahatan CT yang berbentuk unauthorized acces to computer system dan service. Pasal 31 terkait dengan aksi kejahtan Hacking.

Dalam undang-undang ini terkait dengan aksi kejahatan CT yang berbentuk *cyber sabotage* dan *extortion.* Pasal 33 menyangkut aksi kejahatan CT yang berbentuk *unauthorized acces to computer system and service*. Oleh karena itu, nampak bahwa perspektif Undang undang Informasi dan Transaksi Elektronik adalah menekankan pada aspek penggunaan/ keamanan Sistem Informasi Eleketronik atau Dokumen Elektronik, dan penyalahgunaan di bidang teknologi dan transaksi elektronik yang dilakukan oleh para pelaku CT.

- **RUU KUHP**

Sehubungan dengan kelemahan yuridiksi di dalam KUHP dalam menghadapi masalah *Cyber Terorism*, maka dalam konsep RUU KUHP 2004/2005, dirumuskan perluasan asas teritorial, sebagai berikut. Ketentuan Pidana dalam peraturan perundangperundangan Indonesia berlaku bagi setiap orang yang melakukan tindak pidana dibidang teknologi informasi yang akibatnya dirasakan atau terjadi di wilayah Indonesia dan dalam kapal atau pesawat udara Indonesia. Di dalam buku I ketentuan umum dibuat ketentuan mengenai dibuat beberapa pengertian tentang beberapa pengertian yang berkaitan dengan jaringan computer

- **Kerjasama Internasional**

Sistem peradilan pidana tradisional tidak cukup efektif, menghadapi penjahat yang menggunakan teknologi maju yang canggih beroperasi di dunia siber. Hukum tradisional dalam arti hukum positif yang berlaku dalam hal prosedur, investigasi dan cara pembuktian (alat bukti) dalam sidang pengadilan tidak dapat menjawab kebutuhan akan sifat kejahatan dalamdunia siber. Badan-badan penegak hukum juga tidak dapat menyelidiki kejahatan siber dan mengumpulkan bukti dengan baik, sehingga memerlukan pengetahuan tekhnis. Untuk meningkatkan kemampuan bagi penegak hukum tersebut harus diupayakan beberapa langkah positif di level internasional dengan mendidik penegak hukum tentang pengetahuan tekhnis teknologi informasi. Hal tersebut, mengingat sifat kejahatan cyberterrorism yang bersifat global, maka lembaga penyidikan harus bekerjasama dan memiliki hubungan internasional agar proses penyidikan bisa dulakukan secara cepat, efektif dan tepat. Hal ini penting, karena solusi atas cyberterrorism hanya dapat dilakukan di tingkat internasional dan bukan bertumpu hanya pada masing-masing negara.

C. Penutup

Cyber Terrorism merupakan bentuk transformasi terror yang dilakukan oleh teroris dengan menjadikan jaringan internet sebagai alat atau sasaran serangan. Jenis kejahatan ini bermetamorfosis menjadi kejahatan yang bersifat lintas negara. Pelakunya bisa berasal dari wilayah negara mana saja yang berakibat hukum pada identitas yang berimplikasi pada penentuan yurisdiksi pengadilan. Dengan pola yang cukup maju ini maka dibutuhkan upaya

yang komprehensif untuk menanggulanginya baik berupa penguatan instrumen hukum dalam negeri, pemanfaatan teknologi dan kerja sama yang bersifat global atau antarnegara.

Salah satu penyelesaian masalah dari perkara *Cyber Terrorism* ini yaitu hendaknya setiap negara harus melakukan sinkronisasi tentang peraturan perundang-undangan yang khusus mengatur tentang *cyberterror*. Terlihat upaya serius Indonesia dari upaya sinkronisasi beberapa sistem hukum nasional dengan beberapa KUHP asing atau konvensi internasional. Ini untuk dilakukan untuk mengantisipasi masalah penentuan jenis tindak pidana, namun persoalan yurisdiksi masih terkendala. Namun pendekatan represif ini juga harus dilengkapi dengan pemanfaatan teknologi. Pendekatan ini menjadi sangat strategis karena hukum pidana mengandung keterbatasan untuk mengatasi akar penyebab *Cyber Terrorism*.

D. Daftar Pustaka

Arief, Barda Nawawi. 2006. Tindak Pidana Mayantara Perkembangan Kajian CyberCrime diIndonesia. Jakarta : RajaGrafindo Persada

Brenner Susan W. 2007. Cybercrime: Re-Thinking Crime Control Strategies, dalam Yvonne Jewkes (edt). Crime Online. USA: Willan Publishing.

Colarik, Andrew Michael. 2006. Cyber Terrorism: Political and Economic Implications. IdeaGroup: USA

Picard, Janet J. Laurie E. Macdonald. 2004. Cyber Terorism: A study of the extent coverage incomputer security textbook. Journal of Information technology education. Volume 3. 200.

Trachmant. Joel P. 2006. Global Cyberterrorism, Jurisdiction, And International Organization, Dalam Mark F. Grady & Francesco Parisi, The Law And Economics Of Cybersecurity. Cambridge: Cambridge University Press.