KEBIJAKAN ANTISIPATIF HUKUM PIDANA UNTUK PENANGGULANGAN *CYBERTERRORISM*

Ufran
Fakultas Hukum Universitas Mataram
email : ufrantrisa@yahoo.com

Abstract

This article attempts to explain briefly associated with a set of issues relating to cyberterrorism. It also needs to think about the future of criminal law anticipatory policy in the mengelminir cyberterrorism as a trend of crime in the future. Analysis showed that the Cyberterrorism is a form of transformation of terror carried out by terrorists by making the Internet as a tool or target of the attack . This type of crime morphed into a cross- country crime. The culprit could come from any area of the country that legal consequences on the identity of the implications for the determination of the court's jurisdiction. With this advanced enough pattern of cooperation that is needed is globaly. One solution every country must synchronize on legislation that specifically regulates cyberterror .

Keywords: Criminal Policy, Cyberterrorism, State.

Abstrak

Artikel ini berupaya menjelaskan secara ringkas berkaitan dengan seperangkat isu-isu yang berkaitan dengan cyberterrorism. Selain itu juga kedepan perlu dipikirkan tentang kebijakan antisipatif hukum pidana dalam mengelminir terjadinya cyberterrorism sebagai trend of crime kedepan. Analisa menunjukan bahwa Cyberterrorism 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 jurisdiksi pengadilan. Dengan pola yang cukup maju ini maka dibutuhkan kerjasama yang bersifat global atau internegara. Salah satu solusinya setiap negara harus melakukan sinkronisasi tentang peraturan perundang-undangan yang khusus mengatur tentang cyberterror.

Kata Kunci: Kebijakan Pidana, Cyberterrorism, Negara.

A. Latar Belakang

Dunia pada hari ini, telah menjadi lebih terhubung oleh teknologi informasi dan komunikasi daripada sebelumnya. Sistem telekomunikasi dan komputer dapat terhubung secara global (*have global reach),*[1] baik mentransfer suara dan data digital yang melintasi batas-batas negara. Sistem tersebut juga menjadi penggerak untuk mendukung pengembangan infrastruktur ekonomi dan industri transportasi, termasuk perdagangan dan layanan pemerintah.

Manfaat kemajuan teknologi informasi dan komunikasi khususnya internet telah menyentuh semua sisi kehidupan manusia modern. Sisi positif ini ternyata diikuti sisi gelap (*dark side*)[2] penggunaan internet. Internet telah mengalami evolusi, yang semula digunakan untuk kepentingan militer dan ilmiah menjadi sasaran dan sarana kejahatan. Para pengguna internet tidak saja hanya para ilmuwan, pengguna umum melainkan dipakai oleh mata-mata dan teroris.

Melihat ketergantungan yang cukup besar terhadap internet maka serangan teroris yang ditujukan kepadanya menjadi ancaman serius yang termasuk wilayah baru bagi keamanan nasional dan kebijakan publik. Oleh karena itu, ketika suatu negara

[1] Andrew Michael Colarik, *Cyber Terrorism:Political and Economic Implications, USA, Idea Group Publishing,* hlm. xi
[2] Lukasz Jachowicz, *Cyberterrorism And Cyberhooliganism: How To Prevent And Fight International and Domestic*, paper presented at Collegium Civitas Foreign Policy of the United States of America, January 2003, hlm. 1.

ketika ingin beranjak pada *e-link* segala urusan yang bersifat publik sebagai kepentingan nasionalnya maka negara tersebut harus mulai memikirkan untuk mengamankan sistem jaringannya dari serangan, khususnya dari *cyberterrorism*. Maka sangat penting fenomena *cyberterrorism* dipahami dengan baik karena bayang-bayang serangan terorisme yang selalu mengintai kita semua setiap saat.

Sisi lain yang perlu dicermati yaitu adanya kecenderungan dari para ahli yang menganggap *cyberterrorism* sebagai kejahatan dunia siber biasa. Anggapan seperti ini tidak saja menjebak kita untuk bersikap menyederhanakan persoalan melainkan juga berakibat pada kualitas respon antisipatifnya menjadi lamban dan terkesan tidak serius. Padahal jika ditilik secara mendalam penggunaan jaringan internet berkorelasi positif dengan transformasi jaringan teror yang awal keanggotaannya terbatas pada wilayah tertentu berubah menjadi massal dan berskala global.

Untuk itu, diperlukan pemahaman yang memadai mengenai anatomi *cyberterrorism*. Keutuhan pemahaman mengenai kejahatan yang tergolong baru ini menjadi penting untuk membuat peta jalan yang komperehensif untuk meminimalisir kemampuan teroris untuk melakukan serangan terhadap jaringan atau*pun* menjadikan komputer sebagai media untuk propaganda teror. Oleh karena itu, artikel ini berupaya menjelaskan secara ringkas berkaitan dengan seperangkat isu-isu yang berkaitan dengan *cyberterrorism*. Selain itu juga kedepan perlu dipikirkan tentang kebijakan antisipatif hukum pidana dalam mengelminir terjadinya *cyberterrorism* sebagai *trend of crime* kedepan.

B. Pembahasan

1. Kategorisasi Cyberterrorism

Sebelum membahas lebih cara merespon *cyberterrorism* maka penting untuk mendefinisikan beberapa istilah operasional. Istilah-istilah tersebut antara lain "*cyberspace*," "*cybersecurity*," "*cybercrime*," and "*cyberterrorism*." Di dalam makalah ini, istilah "*cyberspace*," secara sederhana dimaksudkan internet itu sendiri, *a network of networks to handle communications between computers*. Aktivitas utama pada *cyberspace* adalah mengakses *web pages* dan berkomunikasi melalui *e-mail*. "*Cybersecurity*" *is a broad term for security against disruption and misuse of Internet facilities*. "*Cybercrime*" *includes a full range of traditional crime effected using the Internet as well as "new" crimes involving criminalized disruption and misuse of the Internet*.[3] "*Cyberterrorism*" adalah sebuah bentuk cybercrime yang dikategorisasikan sebagai terorisme.[4]

Istilah *cyberterror* merupakan istilah yang cukup baru. Federal Bureau of Investigation (FBI) mendefinisikan *cyberterror* sebagai, penggunaan kekuatan yang melanggar hukum atau kekerasan terhadap orang atau properti untuk mengintimidasi atau memaksa pemerintahan, penduduk sipil, atau segmen daripadanya, sebagai kelanjutan dari tujuan politik atau sosial menggunakan/ melalui eksploitasi dari sistem untuk menyerang target.[5]

Definisi tentang *cyberterrorism* dikemukakan oleh James A. Lewis yang mendefinisikan *cyberterrorism* sebagai, 'penggunaan perangkat jaringan komputer untuk mematikan infrastruktur nasional yang cukup penting (seperti energi, transportasi, bekerjanya pemerintahan) atau untuk mengganggu (*coerce*) atau mengintimidasi sebuah pemerintahan atau kelompok warga negara (*civilian population*)'.[6]

Cyberterrorism merupakan tindak pidana yang dilakukan melalui komputer yang mengakibatkan kekerasan, kematian dan/atau kehancuran, dan menciptakan teror untuk tujuan memaksa pemerintah untuk mengubah kebijakannya.[7]

2. Evolusi Menuju *Cyberterrorism*

Sebagaimana dikemukakan pada bagian awal tulisan ini *cyberterrorism* menjadi sisi gelap (*dark*

[3] Susan W. Brenner, 2007, *Cybercrime: Re-Thinking Crime Control Strategies*, dalam Yvonne Jewkes (edt), Crime Online, USA, Willan Publishing, hlm. 13.
[4] Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, And International Organization*, Dalam Mark F. Grady & Francesco Parisi, The Law And Economics Of Cybersecurity, Cambridge, Cambridge University Press 2006, hlm. 261.
[5] *Overview of Cyber-Terrorism*," at www.cybercrimes.net/Terrorism/overview/page1.html, September 21, 2002
[6] James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies (CSIS), December, 2002, hlm. 1
[7] Lukasz Jachowicz, *Cyberterrorism… p. 2*

side) kemajuan teknologi informasi. Pelaku teror atau kelompok teroris dengan kemajuan teknologi informasi kian tumbuh lebih adaptif dan progresif. Mereka menggunakan teknologi informasi/internet untuk menjalankan roda organisasi teror dengan lebih efektif. Implikasinya memungkinkan pengembangan keorganisasian yang sifatnya lokal menjadi kelompok teror transnasional atau *global group terrorism*. Mereka bisa lebih mudah melakukan kordinasi dan perintah kepada sel-sel anggota di seluruh dunia dan kemajuan teknologi informasinya membuka jalan untuk itu. Oleh karena itu, pada bagian ini akan dibahas pergeseran dari tahap ke tahap evolusi terorisme yang serangannya bersifat nyata/ fisik menuju pada serangan mayantara. Secara sederhana Andrew Michael Colarik membagi tiga tahapan perkembangan menuju cyber terrorism. Adapun tiga tahapan tersebut, yaitu: (a) h*ackers to crackers; (b) crackers to cyber criminals, and (c) cyber Criminals to cyber terrorists.*

Secara berbeda tahapan evolusi ini dibagi ke dalam tiga tingkatan kemampuan menuju *cyber terrorism* seperti yang didefinisikan oleh Naval Post-graduate School di Monterey, yang terdiri dari:

a. *Simple-Unstructured*, kemampuan untuk melakukan *hacks* dasar terhadap sistem individu menggunakan alat-alat yang dibuat oleh orang lain.
b. *Advanced-Structured*, kemampuan untuk melakukan serangan yang lebih canggih terhadap beberapa sistem dan mungkin untuk mengubah atau menciptakan alat-alat dasarnya.
c. *Complex-Coordinated*: kemampuan untuk melakukan serangan terkoordinasi yang menyebabkan gangguan massal terhadap banyak sistem pertahanan.[8]

3. Anatomi *Cyber-Terrorism*

Untuk memetakan apa yang dimaksud dengan *cyber terrorism* dengan jenis kejahatan siber lainnya ini[9] alangkah lebih baiknya kita memahami model yang diajukan oleh Bradley K. Ashley di dalam makalahnya yang berjudul *Anatomy Of Cyberterrorism: Is America Vulnerable*? Model ini memetakan anatomi tentang cyber terrorism secara lebih jelas. Adapun model tersebut bisa digambarkan dalam bentuk sebagai berikut:[10]

Model ini menggambarkan anatomi *cyberterrorism*, maka pertama harus dipahami lingkungan dunia maya beserta atributnya yang bersifat unik. Kemudian dengan menganalisis berbagai komponen anatomi *cyberterrorism*, kita dapat memahami jawaban atas pertanyaan dasar: siapa, apa bagaimana, dimana, mengapa, dan kapan. Hanya setelah seseorang memahami pilar-pilar dasar tersebut, seseorang dapat memahami dengan baik tentang cyberterrorism.

Untuk memahami *cyberterrorism*, harus dipelajari komponen dan menganalisa pertanyaan-pertanyaan seperti siapa, apa, bagaimana, dimana, mengapa, dan kapan? Di bawah ini akan diuraikan satu persatu pertanyaan di atas.

a. Pelaku (*Actors*)

Colarik menegaskan, *There is no cyber terrorism without terrorism, period*.[11] Pernyataan

[8] *ibid*
[9] Joel P. Trachtman. *Global cyberterrorism, jurisdiction, and International organization,* dalam Mark F. Grady & Francesco Parisi *(*Edited), 2006, *The Law And Economics Of Cybersecurity,* Cambridge University Press, hlm. 262.
[10] Bradley K. Ashley, *Anatomy Of Cyberterrorism: Is America Vulnerable*?, A Research Paper Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Maxwell AFB, AL, 27 February 2003, p.
[11] Andrew Michael Colarik, *Cyber Terrorism:Political and Economic Implications, USA, Idea Group Publishing,* hlm. 15

tersebut menegaskan bahwa pelaku *cyberterrorism* merupakan para teroris. Mereka melancarkan kegiatan terornya dengan menggunakan fasilitas siber. Penggunaan computer sebagai alat dan sasaran serangan merupakan bentuk penggunaan kekerasan dan intimidasi,[12] khususnya untuk tujuan politik.[13]

b. Tools (*Alat*)

Terjadinya *cyber terrorism* tersebut tentunya dengan premise dasar bahwa infrastruktur penting sebuah negara lebih tergantung pada pemanfaatan jaringan komputer untuk bekerjanya. Para pelaku atau kelompok pelaku melakukan serangan secara masif untuk melakukan penetrasi terhadap jaringan keamanan komputer dan menghilangkan atau mematikan fungsi-fungsi pentingnya

c. Sasaran (*Targets*)

Negara-negara pada seluruh wilayah didunia pada saat ini sangat tergantung pada sistem informasi. Sistem informasi merupakan kebutuhan dasar bagi suatu negara untuk melayani kepentingan publik. kepada rakyat *nya*. Maka serangan cyberterrorism selalu menargetkan sasarannya pada *critical information infrastructure.*[14] Adapun beberapa infrastruktur informasi yang cukup penting yang menjadi sasaran serangan *cyberterrorism* adalah *1. Agriculture; 2. Food; 3. Water; 4. Public health; 5. Emergency services; 6. Government; 7. Defense industrial base; 8. Information and telecommunications; 9. Energy; 10. Transportation; 11. Banking and finance; 12. Chemical industry and hazardous materials; 13. Postal and shipping; 14. Real estate*

d. Motif

Secara umum ada beberapa motif kenapa internet sering menjadi alat atau sasaran tempat terjadinya kejahatan. Menurut Phillip W. Brunst ada beberapa motivasi umum kenapa kejahatan dilakukan di internet. Adapun beberapa faktor-faktor yang menjadi motivasinya yaitu: *1), Location Independence, 2) Speed, 3) Anonymity, 4) Internationality, dan* 5), *Cost-Benefit Ratio*.[15]

Lebih lanjut Brunst menjelaskan lima bentuk motivasi tersebut berlaku bagi kejahatan cyberterrorism atau bagi kejahatan dunia siber biasa lainnya. Perbedaanya bisa diketahui atau diamati sehubungan dengan agenda yang mendasarinya. Tujuan utama teroris adalah melahirkan ketakutan, membuat kepanikan ekonomi atau mendiskriminasi lawan politik. Tujuan lainnya bisa jadi adalah terlepas dari motif utama seperti menurunkan pendapatan moneter atau pengumpulan informasi (baik untuk konvensional atau serangan elektronik).

Sebagai catatan penting, serangan di internet merupakan salah satu cara yang dilakukan untuk mencpai tujuan. Isu terkait dengan ini adalah kesulitan untuk mendeteksi niat teroris di balik aksinya di internet. Dalam perspektif obyektif murni, untuk menggali alasan atau motivasi pelaku serangan sangat sulit dibedakan antara *cybercrime* biasa dan *cyberterrorism* sulit untuk membuat. Untuk analisa ini akan sangat tergantung dari penelusuran kasus dan interkoneksi anatara factor-faktor sehingga bisa diidentifikasi sebagai *cyberterrorism* sebagaimana dijelaskan.

e. Waktu Serangan (*Timing)*

Dari motif kenapa internet menjadi pilihan sebagai alat atau sasaran serangan oleh teroris yang dijelaskan di atas, maka konsekuensi

---

[12] *In the use of force in conventional warfare, we might bomb a portion of our opponent's nfrastructure in order to disrupt their electrical grid. In cyber warfare, use of force could mean the sabotage of a Supervisory Control and Data Acquisition (SCADA) system controlling a portion of the electrical grid, and the subsequent failure of the grid. Although we might never have moved a single combatant, or, in fact, moved from our desk, we have still achieved our goal of disrupting the infrastructure of our opponent. This tends to imply that the term use of force is inadequate, or needs to be redefined, in order to include attacks of a cyber nature.ibid* page 226

[13] The *Oxford Student's Dictionary* dalam Tamar Meisels, *Defining terrorism – a typology, Critical Review of International Social and Political Philosophy*, 12:3, 331-351 To link to this article: http://dx.doi.org/10.1080/13698230903127853

[14] Samuel C. McQuade (Edt.) , 2009, *Encyclopedia Of Cybercrime,* London, Greenwood Press, page 38.

[15] Phillip W. Brunst, *Terrorism and the Internet: New Threats Posed* by Cyberterrorism and Terrorist Use of the Internet, dalam Marianne Wade dan Almir Maljeviæ (Edt) A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications, New York, Springer, page 52-56

logisnya serangan bisa dilakukan kapan saja. Selain faktor-faktor tersebut, maka wwaktu serangan akan sangat ditentukan oleh momentum yang tepat agar ketakutan bisa menyebar luas di kalangan masyarakat. Dengan kata lain, waktu serangan akan berkorelasi dengan tujuan, kemampuan dan faktor rentannya sistema keamanan dari jaringan yang dijadikan alat atau sasaran serangan.

4. Beberapa Upaya Kontrol untuk Meng-antisipasi Cyberterrorism

Cyberterrorism merupakan kejahatan yang cukup sulit untuk dikontrol dan diperangi karena muncul diantara beberapa system hukum. Dengan lokasi dan karakter *cyberterrorism* yang bersifat lintas nasional menjadi kesulitan tersendiri yang berlanjut pada persoalan juridiksi. Persoalannya juga menjadi bertambah yaitu tiadanya kesepahaman hukum tentang jenis perbuatan apa saja digolongkan sebagai tindak pidana di antara berbagai sistem hukum yang ada sehingga menambah berbahayanya gambaran kejahatan ini. Oleh karena itu, pembahasan pada bagian ini mengeksplorasi tentang pendekatan 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 dan pengaturan yang bersifat *inter-state* atau global. Tujuannya agar kebijakan antisipatif hukum pidana menjadi respon terukur dan sistematis sebagai bagian kebijakan yang rasional untuk mengantisipasi *cyberterrorism*.

a. Pendekatan Teknologi (*Techno Prevention*)

Hukum pidana tidak akan mampu bekerja sendiri. Berdasarkan tesis ini maka cara yang harus diutamakan adalah menghilangkan faktor-faktor pada level penyebab atau akar masalah. Seperti dijelaskan pada bagian awal makalah 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 kedepan 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.[16] Untuk menyederhanakan pembahasan, makalah 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 tentang data 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 tentang penyalahgunaan data diri seseorang untuk melakukan serangan teror maka cara antisipatif yang dapat digunakan yaitu mengaktifkan teknologi biometriks.[17] Logika dasar yang dipakai teknologi ini adalah aplikasi

[16] Emily Finch, 2007, *The Problem of Stolen Identity and the Internet,* dalam Yvonne Jewkes (editor), Crime Online, USA, Willan Publishing, hlm 29-32.

[17] Russell G. Smith, 2007, *Biometric Solutions To Identity-Related Cybercrime*, dalam Yvonne Jewkes (editor), Crime Online, USA, Willan Publishing, hlm. 46

teknologi untuk melakukan kontrol dan pembatasan atas akses internet. *Biometric 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 adalah ''*are you who you claim to be*?'

b. Sinkronisasi Legislasi Penal (*Penal Aproach*)

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 ataupun instrument hukum internasional (harmonisasi eksternal/ ke luar).

1). 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. Di bagian tulisan ini, akan disajikan beberapa perspektif kebijakan legislasi di 3 (tiga) negara yaitu Jerman, Belgia dan Estonia. Komparasi ini menjadi penting sebagai bahan perbandingan dan masukan untuk point masukan bagi hukum pidana Indonesia dalam menyikapi *cyberterrorism.*

a) Jerman

Dalam KUHP Jerman (German Penal Code) termuat beberapa ketentuan yang mengatur *cyber crimes and abuse of computer networks*. Adapun beberapa pasal yang berkaitan dengan legislasi atau pengaturan untuk menjadi sumber hukum terhadap *cyberterrorism* terbagi dalam beberapa pasal (*section*) 202 a: *Data Espionage;* 263 a: *Computer fraud*; 269 *Fraud or falsification of legally relevant data;* 270 *Deception or cheating in legal relations through data processing*; 303 a: *Alteration of data,* 303 b: *Computer sabotage*

b) Belgia

Pada bulan November 2000 parlemen Belgia membuat beberapa revisi atau pengaturan tambahan baru terhadap KUHP untuk mengatur beberapa ketentuan *computer forgery, computer fraud and sabotage criminal offence.* Pasal 550 (b) KUHP Belgia mengatur secara khusus *the computer crimes* termasuk dalam beberapa bagian.

c) Estonia

Kitab Undang-Undang Hukum Pidana Estonia mengatur beberapa bagian dalam pengaturan yag bersifat khusus untuk penanggulangan tentang *cyber crimes: S. 269 Destruction or alteration of programmes and data stored in a computer. S. 270 Computer sabotage. S. 271 Unauthorised use of computers, computer system and networks. S. 272 Interfacing or damaging the connections of computer networks. S. 273 Spreading of computer viruses.*

2). Harmonisasi Internal;

Indonesia telah mensahkan 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 yang mengatur teknologi informasi diantaranya, yaitu:

a) 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 dapat diidentifikasikan 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.

b) RUU KUHP

Sehubungan dengan kelemahan yuridiksi di dalam KUHP dalam menghadapi masalah *cyberterorism*, maka dalam konsep RUU KUHP 2004/2005, dirumuskan perluasan asas teritorial, sebagai berikut. Ketentuan Pidana dalam peraturan perundang-perundangan 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 komputer.[18] Di dalam buku II (Tindak Pidana): Dilakukan perubahan perumusan delik atau menambah delik-delik baru yang berkaitan dengan kemajuan teknologi, dengan harapan dapat juga menjaring kasus-kasus *cyberterorism*, di atur dalam Bab V Tindak Pidana Terhadap Ketertiban Umum, antara lain: 1. Menyadap pembicaraan diruangan tertutup dengan alat bantu atau tekhnis (pasal 263/300); 2. Memasang alat bantu tekhnis untuk tujuan mendengar / merekam pembicaraan (pasal 264/301); 3. Merekam (memiliki/menyiarkan) gambar dengan alat bantu tekhnis di ruangan untuk umum (pasal 266/303); Bab VII (Tindak Pidana Yang membahayakan Kepentingan Umum bagi Orang, Barang, dan Lingkungan Hidup): 1. mengakses komputer tanpa hak (pasal. 368,371, 372, 373 konsep 2004); 2. merusak/membuat tidak dapat dipakai bangunan atau sarana/ prasarana pelayanan umum (al. bangunan komunikasi/ komunikasi lewat satelit/komunikasi jarak jauh) pasal. 630/ 2004;

c). 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 dalam dunia siber. Badan-badan penegak hukum juga tidak dapat menyelidiki kejahatan siber dan mengumpulkan bukti dengan baik, sehingga memerlukan pengetahuan tekhnis. Untuk meningkatkan

[18] Barda Nawawi Arief, 2001, "Antisipasi Penanggulangan Cyber Crime Dengan Hukum Pidana", makalah pada Seminar Nasional Mengenai *Cyber Law*, Bandung, STHB

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.[19]

Cyberterrorism tidak saja menjadi masalah yang bersifat nasional melainkan menjadi masalah yang bersifat internasional. Kejahatan ini mendapatkan perhatian yang cukup luas. Kongres PBB ke 8 di Havana, Kongres ke X di Wina, kongres XI 2005 di Bangkok, berbicara tentang *The Prevention of Crime and the Treatment of Offender*. Dalam Kongres PBB X tersebut dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan ketentuan yang berhubungan dengan kriminalisasi, pembuktian dan prosedur (*States should seek harmonization of relevan provision on criminalization, evidence, and procedure*) 21 dan negara-negara Uni Eropa yang telah secara serius mengintegrasikan regulasi yang terkait dengan pemanfaatan teknologi informasi ke dalam instrumen hukum positif (*existing law*) nasionalnya.[20] *The Convention on Cybercrime is intended to improve law enforcement's ability to react to cybercrime* (Council of Europe, 2001). *It seeks to achieve this by: (1) harmonising the domestic criminal substantive law . . . in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences . . . (and) (3) setting up a fast and effective regime of international co-operation.*[21]

Selain upaya-upaya yang dilakukan oleh PBB untuk menggalang kerjasama internasional untuk menanggulangi *cyberterrorism* dan menemukan solusi atas masalah-masalah pelaporan, investigasi, temuan, dan perbaikan cara pembuktian. Muncul beberapa organisasi yang berinisiatif untuk membuat lembaga-lembaga yang bersifat global untuk melawan *cyber crime* khususnya *cyberterrorism.* Adapun lembaga tersebut seperti, *International Services on Discovery and Recovery of Electronic and Internet Evidences, International Organisation on Computer Evidence* (IOCE),[22] GECD Initiatives,[23] Efforts of G-7 and G-8 Groups.

C. Simpulan

Cyberterrorism 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 jurisdiksi pengadilan. Dengan pola yang cukup maju ini maka dibutuhkan kerjasama yang bersifat global atau intemegara. Salah satu solusinya setiap negara harus melakukan sinkronisasi tentang peraturan perundang-undangan yang khusus mengatur tentang *cyberterror.*

---

[19] Laws on Cyber Crimes: Alongwith IT Act and Relevant Rules, Jain Bhawan, Book Enclave, 2007, hlm. 120

[20] Barda Nawawi Arief. *Tindak Pidana Mayantara*, *Perkembangan Kajian CyberCrime di Indonesia*, Jakarta, PT. Raja grafindo Persada, hlm. v

[21] Brenner, 2004, Dalam Susan W. Brenner, *Cybercrime: Re-Thinking Crime Control Strategies*, dalam Yvonne Jewkes (edt) , 2007, Crime Online, USA, Willan Publishing, hlm. 18.

[22] The International Organisation on Computer Evidence (IOCE) was established in 1995 to provide international law enforcement agencies a forum for the exchange of information concerning computer crime ivnestigation and other computer related forensic issues.

[23] *Organisation for Economic Cooperation and Development (OECD) was set up in 1983 in Paris for initiating an international effort in harmosing the legal responses towards cyber crimes. OECD in the international conference discussed computer related crime and the need for changes in the penal codes of the member countries. OECD recommended member countries to bring in necessary changes in their penal legislation to cover certain types of cyber crimes.*

Terlihat upaya serius Indonesia dari upaya sinkronisasi beberapa system hukum nasional dengan beberapa KUHP asing atau konvensi internasional. Ini untuk dilakukan untuk mengantisipasi masalah penentuan jenis tindak pidana, namun persoalan jurisdiksi masih terkendala. Namun pendekatan represif ini juga harus dilengkapi dengan pendekatan teknologis. Pendekatan ini menjadi sangat strategis karena hukum pidana mengandung keterbatasan untuk menjawab soal akar penyebab *cyberterrorism.*

DAFTAR PUSTAKA

Arief, Barda Nawawi, 2001, "Antisipasi Penanggulangan Cyber Crime Dengan Hukum Pidana", makalah pada Seminar Nasional Mengenai Cyber Law, Bandung: STHB.

Arief, Barda Nawawi, 2009, *Tindak Pidana Mayantara*, Perkembangan Kajian CyberCrime di Indonesia, Jakarta: PT. Raja grafindo Persada.

Ashley, Bradley K., "Anatomy Of Cyberterrorism: Is America Vulnerable?", A Research Paper Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, Maxwell AFB, AL, 27 February 2003.

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

Brunst, Phillip W. *Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet*, dalam Marianne Wade dan Almir Maljeviæ (Edt), 2013, A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications, New York: Springer.

Colarik, Andrew Michael , 2006, *Cyber Terrorism: Political and Economic Implications*, USA: Idea Group Publishing.

Finch, Emily, *The Problem of Stolen Identity and the Internet*, dalam Yvonne Jewkes (editor), 2007, Crime Online, USA: Willan Publishing.

Janczewski, Lech J. dan Andrew M. Colarik (edt) , 2008, *Cyber Warfare and Cyber Terrorism,* USA: Information Science Reference.

Lewis, James A., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies (CSIS), December, 2002.

Lukasz Jachowicz, "Cyberterrorism And Cyberhooliganism: How To Prevent And Fight International and Domestic, paper presented at Collegium Civitas Foreign Policy of the United States of America", January 2003.

McQuade, Samuel C. (Edt.)*, 2009, Encyclopedia Of Cybercrime,* London: Greenwood Press.

Meisels, Tamar, *Defining terrorism – a typology, Critical Review of International Social and Political Philosophy,* 12:3, 331-351 To link to this article: http://dx.doi.org/10.1080/13698230903127853

Nagpal, Rohas, 2007, *Laws on Cyber Crimes: Alongwith IT Act and Relevant Rules*, Jain Bhawan: Book Enclave.

Overview of Cyber-Terrorism," at www.cybercrimes.net/ Terrorism/overview/page1.html, September 21, 2002.

Smith, Russell G., *Biometric Solutions To Identity-Related Cybercrime*, dalam Yvonne Jewkes (editor) , 2007, Crime Online, USA: Willan Publishing.

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