KEJAHATAN TRANSNASIONAL DALAM *CYBER TERRORISM* MENURUT UNDANG– UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK[1]

Oleh : Ria Anggraini Wijaya[2]
Dosen Pembimbing:
Max K. Sondakh, SH. MH.
Dr. Natalia L. Lengkong, SH., MH.

ABSTRAK

Penelitian ini dilakukan dengan tujuan untuk mengetahui bagaimana pengaturan mengenai *cyber terrorism* sebagai kejahatan transnasional dan bagaimana merumuskan delik terhadap pelaku tindak pidana *cyber terrorism* menurut Undang – Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik serta bagaimana penerapan Undang – Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik terhadap pelaku tindak pidana *cyber terrorism* yang berkedudukan warga negara asing. Dengan menggunakan metode penelitian yuridis normatif, disimpulkan: 1. Pengaturan mengenai *cyber terrorism* sebagai kejahatan transnasional belum terdapat pengaturan secara khusus terkait *cyber terrorism* dalam hukum internasional. Dalam situasi kekosongan hukum ini, *ASEAN Convention on Counter Terrorism* dan *International Convention for the Suppression of Terrorist Bombings* mulai dipergunakan sebagai dasar hukum untuk mempidanakan pelaku *cyber terrorism. ASEAN Convention on Counter Terrorism* telah diratifikasi oleh Indonesia melalui Undang-undang Nomor 5 tahun 2012 tentang Pengesahan *ASEAN Convention on Counter Terrorism*, sedangkan *International Convention for the Suppression of Terrorist Bombings* diratifikasi melalui Undang-undang Nomor 5 tahun 2006 tentang Pengesahan *International Convention for the Suppression of Terrorist Bombings.* Sedangkan dalam pengaturan menurut hukum nasional Indonesia, pengaturan yang terkait dengan *cyber terrorism*, yaitu Amandemen Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, amandemen Undang-undang Nomor 15 tahun 2003 Jo. Perpu No. 1 tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme, dan ketentuan penanggulangan terorisme dan pendanaan terorisme diintegrasikan dalam Rancangan Kitab Undang-undang Hukum Pidana yang baru. 2. Dalam Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat ketentuan pasal-pasal, yaitu Bab 11 mengenai ketentuan pidana yang dapat di identifikasi perbuatan yang dilarang (unsur tindak pidana) yang erat kaitannya dengan tindak pidana *cyber terrorism* pada tiap-tiap pasalnya. Seperti pasal 30 terkait dengan aksi kejahatan *cyber terrorism* yang berbentuk *cyber sabotage* dan *extortion* (kejahatan sabotase atau pemerasan). Serta pasal 33 menyangkut aksi kejahatan *cyber terrorism* yang berbentuk *unauthorized acces to computer system and service* (kejahatan yang dilakukan dengan memasuki/ menyusup ke dalam suatu sistem jaringan komputer secara tidak sah. 3. Dalam penerapan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diberlakukan terhadap pelaku yang berkedudukan warga negara asing berdasarkan Pasal 2.

Kata kunci: Kejahatan, transnasional, *cyber terrorism*,

PENDAHULUAN

A. Latar Belakang Masalah

Internet sebagai salah satu alat komunikasi memudahkan teroris untuk mengatur rencana, memberikan arahan, mengontrol maupun interaksi dengan anggota kelompok. Tahun 2008, serangan bom di Mumbai terbukti menggunakan *Voice Over Internet Protocol* (VOIP) untuk aksi teror dan komunikasi antar anggota teroris. Begitu juga dengan perencanaan Bom WTC pada tahun 2001 dengan fasilitas internet berupa pesan yang telah di enkripsi menggunakan sandi rahasia yang dikirim melalui *e-mail* dari warung internet (warnet), perpustakaan atau tempat umum lainnya.[3]

Dengan kata lain, *cyber terrorism* dinyatakan sebagai kejahatan transnasional

[1] Artikel Skripsi.
[2] Mahasiswa pada Fakultas Hukum Unsrat, NIM. 14071101641

[3] Petrus Reinhard Golose, 2015, *Invasi Terorisme Ke Cyberspace,* Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian, hlm 79-80.

yang 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.[4] Kejahatan yang dilakukan para pelaku *cyber terrorism*, yaitu berupa serangan. Serangan tersebut berbeda halnya dengan **serangan** yang dilakukan para pelaku *cyber crime*. Dalam serangan *cyber terrorism* ini, 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. Sedangkan serangan *cyber crime*, yaitu berupa serangan pada sistem elektronik.[5]

Dalam ketentuan hukum *cyber crime* sendiri diatur dalam Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di mana undang – undang ini juga dapat menjerat pelaku tindak pidana *cyber terrorism*. Seperti yang telah dikatakan sebelumnya bahwa *cyber terrorism* dapat dilakukan oleh siapa saja dan tidak menutup kemungkinan kejahatan ini juga dapat dilakukan oleh pelaku yang berkedudukan warga negara asing.

Asas legalitas atau peraturan perundang-undangan tidak disebutkan untuk tidak boleh melakukan penafsiran hukum terhadap rumusan delik yang ada pada peraturan perundang-undangan. Sehingga apabila terjadi tindak pidana *cyber terrorism* dapat dilakukan penafsiran hukum terhadap rumusan delik yang ada pada peraturan perundang – undangan dalam hal ini, diantaranya Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Keterlibatannya teroris yang selalu memunculkan kejahatannya melalui internet dengan melintasi batas negara justru menimbulkan pertanyaan bagaimana pengaturan mengenai *cyber terrorism* sebagai bentuk dari kejahatan transnasional, bagaimana penerapan Undang - Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diberlakukan untuk menjerat pelaku tindak pidana *cyber terrorism* yang berkedudukan warga negara asing. Lalu bagaimanakah merumuskan delik terhadap pelaku tindak pidana *cyber terrorism* di Indonesia menurut Undang – Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Berdasarkan uraian tersebut serta didorong keinginan untuk memperdalam pemahamam tentang Kejahatan Transnasional dalam *Cyber Terrorism*, maka penulis tertarik untuk menulis skripsi dengan judul Kejahatan Transnasional dalam *Cyber Terrorism* menurut Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

B. Rumusan Masalah

1. Bagaimana pengaturan mengenai *cyber terrorism* sebagai kejahatan transnasional?
2. Bagaimana merumuskan delik terhadap pelaku tindak pidana *cyber terrorism* menurut Undang – Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik?
3. Bagaimana penerapan Undang – Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik terhadap pelaku tindak pidana *cyber terrorism* yang berkedudukan warga negara asing?

C. Metode Penelitian

Penelitian yang dilakukan adalah penelitian hukum normatif dimana penelitian tersebut merupakan penelitian perpustakaan yang melakukan kajian studi dokumen, pengumpulan data-data sekunder seperti Peraturan Perundang-undangan, teori-teori hukum dan pendapat-pendapat dari Sarjana. Karena penelitian ini menggunakan pendekatan normatif, maka penelitian ini menitik beratkan pada penelitian kepustakaan yakni dengan melakukan pendekatan kepada Peraturan Perundang-undangan dan studi kasus. Pendekatan tersebut dilakukan dengan menelaah semua undang-undang dan kasus-kasus yang bersangkutan dengan masalah yang dibahas dalam penelitian ini. Dalam

[4] Alfira Nurliliani Samad, 2014, "Analisis Instrumen Cyber Terrorism Dalam Kerangka Sistem Hukum Internasional" (Fakultas Hukum Universitas Hasanuddin Makassar), hlm 37.
[5] *Ibid*., hlm. 38.

metode penelitian hukum normatif ini, terdapat 3 bahan pustaka atau data sekunder yakni bahan hukum primer, sekunder dan tersier.

PEMBAHASAN

A. Pengaturan mengenai *Cyber Terrorism* sebagai Kejahatan Transnasional

Hingga saat ini belum terdapat pengaturan secara khusus terkait *cyber terrorism* dalam hukum internasional. Dalam situasi kekosongan hukum ini, *ASEAN Convention on Counter Terrorism* dan *International Convention for the Suppression of Terrorist Bombings* kiranya dapat dipergunakan sebagai dasar hukum untuk mempidanakan pelaku *cyber terrorism*. *ASEAN Convention on Counter Terrorism* telah diratifikasi oleh Indonesia melalui Undang-undang Nomor 5 tahun 2012 tentang Pengesahan *ASEAN Convention on Counter Terrorism* sedangkan *International Convention for the Suppression of Terrorist Bombings* diratifikasi melalui Undang-undang Nomor 5 tahun 2006 tentang Pengesahan *International Convention for the Suppression of Terrorist Bombings.*[6]

Ketiadaan konvensi internasional yang khusus mengatur mengenai *terrorism* mengundang komentar seorang hakim Mahkamah International (ICJ) berkebangsaan Inggris, Rossalyn Higgins dan sarjana lainnya seperti Maurice flory berpendapat bahwa usaha untuk membentuk hukum positif baru guna menangani kasus-kasus terorisme akan mengundang perdebatan panjang mengenai definisi dan tipologi terorisme.[7]

Meskipun belum memuat secara khusus aturan mengenai *cyber terrorism,* terminologi *cyber terrorism* mulai dipergunakan *ASEAN Convention on Counter Terrorism. Article VI (1) (j)* konvensi tersebut menyatakan sebagai berikut:[8]

> -*"The areas of cooperation under this Convention may, in conformity with the domestic laws of the respective Parties, include appropriate measures, among others, to: … Strengthen capability and readiness to deal with chemical, biological, radiological, nuclear (CBRN) terrorism,* ***cyber terrorism*** *and any new forms of terrorism;*
>
> (Bidang kerjasama berdasarkan Konvensi ini dapat, sesuai dengan hukum domestik masing-masing pihak, termasuk tindakan yang tepat, di antara yang lain, untuk: ... Memperkuat kemampuan dan kesiapan untuk menangani bahan kimia, terorisme biologis, radiologi, nuklir (CBRN), *cyber terrorism* dan apapun bentuk-bentuk terorisme baru).

Sayangnya, konvensi tersebut tidak mengatur lebih lanjut mengenai unsur-unsur tindak pidana *cyber terrorism,* ruang lingkup *cyber terrorism*, serta apa yang membedakannya dengan tindak pidana terorisme.[9] Oleh sebab itu, perlunya dilakukan suatu upaya hukum yang dapat menyelaraskan dan menyesuaikan peraturan-peraturan yang ada dengan instrumen hukum internasional. Upaya ini disebut dengan upaya harmonisasi, harmonisasi hukum merupakan salah satu kegiatan ilmiah yang dilakukan dalam usaha untuk menuju proses penyerasian dan penyelarasan di antara peraturan perundang-undangan yang ada sebagai suatu bagian integral atau sub sistem dari sistem hukum yang pada akhirnya bertujuan untuk mencapai tujuan hukum.[10]

Harmonisasi pengaturan hukum mengenai *cyber terrorism* amat penting untuk dilakukan karena peraturan perundang-undangan nasional tidak boleh bertentangan dengan hukum internasional. Harmonisasi tetap harus dilakukan walaupun baik dalam hukum internasional maupun hukum nasional belum mengatur secara spesifik mengenai *cyber terrorism.* Adapun substansi yang perlu dilakukan harmonisasi adalah mengenai penyebutan *cyber terrorism* serta pengertiannya*,* ruang lingkup kejahatannya, maupun sanksi yang dijatuhkan kepada pelaku.[11]

Majelis Umum PBB mengeluarkan Resolusi 60/288 tertanggal 20 September 2006 yang berisi tentang *UN Global Counter Terrorism Strategy* (UNNGCTS) dimana terdapat empat pilar strategi global pemberantasan terorisme yang meliputi: (1) pencegahan kondisi kondusif

[6] *Ibid*., hlm. 4.
[7] Dikdik M. Arief Mansur dan Elisatris Gultom, *Loc.Cit*., 76.
[8] Ari Mahartha dan Made Mahartayasa, *Loc.Cit*., 4.
[9] *Ibid*., hlm. 4.
[10] *Ibid*.
[11] *Ibid*., hlm. 5.

penyebaran terorisme; (2) langkah pencegahan dan memerangi terorisme; (3) peningkatan kapasitas negara-negara anggota untuk mencegah dan memberantas terorisme serta penguatan peran sistem PBB; dan (4) penegakan HAM bagi semua pihak dan penegakan *rule of law* sebagai dasar pemberantas terorisme.[12]

B. Rumusan Delik terhadap Tindak Pidana *Cyber Terrorism* Menurut Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang – Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat rumusan delik yang dapat digunakan untuk menjerat pelaku tindak pidana *cyber terrorism* di antaranya:

A. Pasal 27 Ayat (4) Undang – Undang Nomor 11 Tahun 2008

   Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/ atau mentransmisikan dan/ atau membuat dapat di aksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan pemerasan dan/ atau pengancaman.

   Unsur-unsur pasal tersebut adalah sebagai berikut:

   1) Setiap orang;
   2) Dengan sengaja dan tanpa hak;
   3) Mendistribusikan dan/ atau mentransmisikan dan/ atau membuat dapat di aksesnya Informasi Elektronik dan/ atau;
   4) Dokumen Elektronik yang memiliki muatan pemerasan dan/ atau;
   5) Pengancaman.

   Bentuk dalam pasal tersebut sifatnya adalah alternatif yang mana cukup dengan memenuhi rumusan mendistribusikan, mentransmisikan, dan/ atau membuat di aksesnya Informasi Elektronik. Apabila salah satunya terpenuhi maka cukup bahwa perbuatan tersebut memenuhi pasal ini. Selain itu dalam pasal ini termasuk ke dalam delik formil karena dalam pasal ini yang tegas dilarang adalah perbuatannya.[13]

B. Pasal 28 Ayat (2) Undang – Undang Nomor 11 Tahun 2008

   Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/ atau kelompok masyarakat tertentu berdasarkan atau suku, agama, ras dan antar golongan (SARA).

   Pasal di atas memiliki unsur-unsur sebagai berikut:

   1) Setiap orang
   2) Dengan sengaja dan tanpa hak
   3) Menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/ atau kelompok masyarakat tertentu
   4) Berdasarkan atas suku, agama, ras, dan antar golongan (SARA)

C. Pasal 30 Ayat (1) dan (3) jo pasal 33 Undang – Undang Nomor 11 Tahun 2008

   1) Pasal 30 ayat (1)

      Setiap orang dengan sengaja dan tanpa haka tau melawan hukum mengakses Komputer dan/ atau Sistem Elektronik milik orang lain dengan cara apapun.

      Pasal tersebut unsur-unsurnya sebagai berikut:

      a) Setiap orang
      b) Dengan sengaja dan tanpa hak atau
      c) Melawan hukum
      d) Mengakses komputer dan/ atau
      e) Sistem Elektronik milik orang lain dengan cara apapun.

D. Pasal 33 Undang – Undang Nomor 11 Tahun 2008

   Setiap orang dengan sengaja dan tanpa haka tau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/ atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

   Pasal di atas unsur-unsurnya sebagai berikut:

   a) Setiap orang

[12] Petrus Reinhard Golose, *Loc.Cit.,* 179.

[13] Hafidz Putera Nugraha, 2014, "Analisis Yuridis Rumusan Delik tentang Tindak Pidana Cyber Terrorism Ditinjau Undang-undang Nomor 15 tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme dan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik" (Fakultas Hukum Universitas Sebelas Maret Surakarta), hlm. 55.

b) Dengan sengaja dan tanpa hak atau melawan hukum
c) Melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/ atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

E. Pasal 31 Ayat (2) jo Pasal 35 Undang – Undang Nomor 11 Tahun 2008

Setiap orang dengan sengaja dan tanpa haka tau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/ atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/ atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/ atau penghentian Informasi Elektronik dan/ atau Dokumen Elektronik yang sedang ditransmisikan.

Pasal tersebut unsur-unsurnya adalah sebagai berikut:

a) Setiap orang
b) Dengan sengaja dan tanpa hak atau melawan hukum
c) Melakukan intersepsi atas transmisi Informasi Elektronik dan/ atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/ atau Sistem Elektronik tertentu milik orang lain
d) Baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/ atau penghentian Informasi Elektronik dan/ atau Dokumen Elektronik yang sedang ditransmisikan.

F. Pasal 35 Undang – Undang Nomor 11 Tahun 2008

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan menipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/ atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang di otentik.

Pasal tersebut unsur-unsurnya adalah sebagai berikut:

a) Setiap orang
b) Dengan sengaja dan tanpa hak atau melawan hukum
c) Melakukan menipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/ atau Dokumen Elektronik
d) Dengan tujuan agar Informasi Elektronik dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang di otentik.

G. Pasal 30 Ayat (2) jo Pasal 32 Ayat (2) Undang - Undang Nomor 11 Tahun 2008

1. Pasal 30 Ayat (2)

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau Sistem Elektronik dengan cara apapun dengan tujuan utnuk memperoleh Informasi Elektronik dan/ atau Dokumen Elektronik.

Pasal tersebut memiliki unsur-unsur sebagai berikut:

a. Setiap orang
b. Dengan sengaja dan tanpa hak atau
c. Melawan hukum mengakses Komputer; dan/ atau
d. Sistem Elektronik dengan cara apapun dengan tujuan utnuk memperoleh Informasi Elektronik dan/ atau Dokumen Elektronik.

C. Penerapan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik terhadap Tindak Pidana *Cyber Terrorism* yang Berkedudukan Warga Negara Asing

Penerapan Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diberlakukan terhadap pelaku yang berkedudukan warga negara asing. Hal ini dapat dilihat dari perihal yurisdiksi dimuat di dalam Pasal 2 Undang - Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai berikut:

"Undang – undang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang – undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang memiliki akibat hukum di

wilayah hukum Indonesia dan/ atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia".

Undang – undang Nomor 11 Tahun 2008 tentang Infromasi dan Transaksi Elektronik memiliki jangkauan yurisdiksi tidak semata – mata untuk perbuatan hukum yang berlaku di Indonesia dan/ atau dilakukan oleh warga negara Indonesia maupun warga negara asing atau badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal. [14] Pemahaman dari pengertian "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.[15]

Untuk itu penjeratan pelaku tindak pidana *cyber terrorism* baik itu berkedudukan warga negara Indonesia maupun warga negara asing dapat dijerat dalam Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dengan menggunakan undang – undang ini dapat digunakan sebatas pasal – pasal yang dapat mendukung untuk menjerat pelaku tindak pidana *cyber terrorism*. Akan tetapi, di dalam undang – undang tersebut ternyata memiliki kelemahan – kelemahan yang tidak dapat digunakan dalam menanggulangi tindak pidana *cyber terrorism*. Penjelasan mengenai hal tersebut adalah sebagai berikut:

Unsur ancaman pada Pasal 27 Ayat (4) Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> 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 pemerasan dan/ atau pengancaman.

Pasal 6 Undang – Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme:

> Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal, dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran terhadap objek – objek vitalyang strategis atau lingkungan hidup atau fasilitas public atau fasilitas internasional, di pidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 4 (empat) tahun dan paling lama 20 tahun.

Pasal 7 Undang – Undang Nomor 15 Tahun 2003:

> Setiap orang dengan sengaja menggunakan kekerasan atau ancaman kekerasan bermaksud untuk menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau untuk menimbulkan kerusakan atau kehancuran terhadap objek – objek vital yang strategis, atau lingkungan hidup, atau fasilitas publik, atau fasilitas internasional, di pidana dengan pidana penjara paling lama seumur hidup.

Dalam Undang – Undang Informasi dan Transaksi Elektronik tidak dijelaskan lebih lanjut mengenai batasan dari ancaman dalam pasal ini, sehingga mengartikan mengenai ancaman dalam hal ini dapat di pahami dengan cara yang berbeda – beda tergantung orang untuk menafsirkan unsur ini seperti apa. Dalam pasal ini unsur ancamannya tidak jelas dan sangat luas sekali mengenai bentuk ancamannya. Bahwa dengan begitu luasnya arti unsur ancaman ini maka disisi lain dapat menjangkau setiap bentuk ancaman yang diterima oleh orang setiap bentuk yang dianggap orang itu sebagai ancaman kepada dirinya namun di sisi lain pasal 6 dan 7 mengenai terorisme dapat dihubungkan dengan pasal ini karena luasnya penafsiran ini namun disisi lain dapat meloloskan pelaku tindak pidana *cyber terrorism* karena anggapan tiap orang mengenai ancaman berbeda sehingga apabila pelaku dapat membuktikan dia tidak melakukan ancaman melalui media internet dalam dunia maya maka pelaku *cyber terrorism* dapat lolos. [16]

[14] *Ibid*.
[15] *Ibid*.
[16] Hafidz Putera Nugraha, *Loc.Cit*., 89.

Kelemahan lainnya, tidak memberikan definisi secara gramatikal mengenai *cyber terrorism* dan tidak mencantumkan delik percobaan dalam Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pada dasarnya undang – undang yang memuat mengenai pasal pidana merupakan suatu peraturan yang khusus *Lex Specialis Derogat Legi Generalis* artinya adalah bahwa peraturan khusus dapat mengalahkan peraturan umum sehingga jika mengacu kepada asas di atas maka peraturan khusus itu harusnya lebih lengkap dan lebih teliti dalam isi substansinya terutama deliknya sehingga harusnya dicantumkan juga mengenai delik percobaan dalam undang – undang tersebut. [17] Dengan demikian, penerapan Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik masih terbilang lemah karena belum mengatur secara jelas dan terperinci mengenai tindak pidana *cyber terrorism* sehingga menimbulkan ketidakpastian hukum dan kekosongan hukum terhadap tindak pidana ini.[18]

PENUTUP

A. KESIMPULAN

1. Pengaturan mengenai *cyber terrorism* sebagai kejahatan transnasional belum terdapat pengaturan secara khusus terkait *cyber terrorism* dalam hukum internasional. Dalam situasi kekosongan hukum ini, *ASEAN Convention on Counter Terrorism* dan *International Convention for the Suppression of Terrorist Bombings* mulai dipergunakan sebagai dasar hukum untuk mempidanakan pelaku *cyber terrorism. ASEAN Convention on Counter Terrorism* telah diratifikasi oleh Indonesia melalui Undang-undang Nomor 5 tahun 2012 tentang Pengesahan *ASEAN Convention on Counter Terrorism*, sedangkan *International Convention for the Suppression of Terrorist Bombings* diratifikasi melalui Undang-undang Nomor 5 tahun 2006 tentang Pengesahan *International Convention for the Suppression of Terrorist Bombings.* Sedangkan dalam pengaturan menurut hukum nasional Indonesia, pengaturan yang terkait dengan *cyber terrorism*, yaitu Amandemen Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik atau melengkapi rancangan undang-undang Tindak Pidana Teknologi Informasi (UU TiPiTI), amandemen Undang-undang Nomor 15 tahun 2003 Jo. Perpu No. 1 tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme, dan ketentuan penanggulangan terorisme dan pendanaan terorisme diintegrasikan dalam Rancangan Kitab Undang-undang Hukum Pidana yang baru.
2. Dalam Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik terdapat ketentuan pasal-pasal, yaitu Bab 11 mengenai ketentuan pidana yang dapat di identifikasi perbuatan yang dilarang (unsur tindak pidana) yang erat kaitannya dengan tindak pidana *cyber terrorism* pada tiap-tiap pasalnya. Seperti pasal 30 terkait dengan aksi kejahatan *cyber terrorism* yang berbentuk *cyber sabotage* dan *extortion* (kejahatan sabotase atau pemerasan). Serta pasal 33 menyangkut aksi kejahatan *cyber terrorism* yang berbentuk *unauthorized acces to computer system and service* (kejahatan yang dilakukan dengan memasuki/ menyusup ke dalam suatu sistem jaringan komputer secara tidak sah). Jadi Undang-undang ini menekankan pada aspek penggunaan/ keamanan Sistem Informasi Elektronik atau Dokumen Elektronik, dan penyalahgunaan di bidang teknologi dan transaksi elektronik yang dilakukan oleh para pelaku *cyber terrorism*.
3. Dalam penerapan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dapat diberlakukan terhadap pelaku yang berkedudukan warga negara asing berdasarkan pasal 2, pasal ini menjelaskan dengan adanya perbuatan hukum yang melanggar aturan yang sudah ditetapkan pasal tersebut. Dalam undang-undang ini berlaku untuk setiap orang yang melanggar aturan tersebut

[17] *Ibid*., hlm. 90.
[18] Agis Josianto Adam, *Loc.Cit*., 171.

baik orang itu yang berada di wilayah hukum Indonesia maupun yang di luar wilayah hukum Indonesia dan setiap orang yang melanggar hukum tersebut memiliki aturan hukum yang berlaku di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang diakibatkan dari penyalahgunaan Undang-undang Infromasi dan Transaksi Elektronik ini.

B. SARAN

Kejahatan *cyber terrorism* adalah bentuk kejahatan baru yang tentu saja membutuhkan suatu aturan untuk mengendalikan atau memberantas kejahatan tersebut. Oleh sebab itu, Pemerintah Republik Indonesia sebaiknya membuat peraturan perundang – undangan yang khusus mengenai tindak pidana *cyber terrorism* atau melakukan perubahan terhadap Undang – Undang Nomor 11 tahun 2008 tentang Infomrsi dan Transaksi Elektronik mengingat bahwa undang – undang ini dapat digunakan sebatas pasal – pasal yang dapat mendukung untuk menjerat pelaku tindak pidana *cyber terrorism,* ini berarti tidak semua pasal yang mengatur tentang *cyber terrorism* dan di dalam undang – undang tersebut ternyata memiliki kelemahan – kelemahan yang tidak dapat digunakan dalam menanggulangi tindak pidana *cyber terrorism*. Maka dari itu, tindakan tersebut perlu dilakukan oleh pemerintah Indonesia karena apabila di lihat sekarang tindak pidana ini sangat potensial terjadi di Indonesia. Hal ini di karenakan kemajuan teknologi dalam kehidupan masyarakat.

DAFTAR PUSTAKA

Panjaitan, Basaria., 2017, *Mengungkap Jaringan Kejahatan Transnasional*, Refika Aditama, Bandung.

SB, Agus., 2016, *Deradikalisasi Dunia Maya : Mencegah Simbiosis Terorisme dan Media*, Daulat Press, Jakarta.

Purwawidada, Fajar., 2014, *Jaringan Baru Teroris Solo*, Kepustakaan Populer Gramedia, Jakarta.

Prasetyo Dedi dan Panca R.Z serta Widodo Urip, 2016, *Ilmu dan Teknologi Kepolisisan : Implementasi Penanggulangan Terorisme dan Radikalisme Di Indonesia*, PT. Rajagrafindo Persada, Jakarta.

Mansur M. Arief Dikdik dan Gultom Elisatris, 2009, *Cyber Law Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung.

Golose Reinhard Petrus, 2015, *Invasi Terorisme Ke Cyberspace*, Yayasan Pengembangan Kajian Ilmu Kepolisian, Jakarta.

Chazawi Adami dan Ferdian Ardi, 2015, *Tindak Pidana Informasi dan Transaksi Elektronik : Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*, Media Nusa Creative, Malang.

Kaligis O.C, 2012, *Penerapan Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dalam Prakteknya*, Yarsif Watampone, Jakarta.

Sumber Perundang-undangan:

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme

United Nation convention against Transnational Organized Crime 2000

ASEAN Convention on Counter Terrorism

International Convention for the Suppression of Terrorist Bombings

Sumber-sumber Lain :

Olii Irvan Mohammad, (2005). *Sempitnya Dunia Luasnya Kejahatan Sebuah Telaah Ringkas tentang Transnational Crime*, No. 1, September 2008.

Samad, Nurliliani Alfira, (2014). *Analisis Instrumen Cyber Terrorism Dalam Kerangka Sistem Hukum Internasional*, Fakultas Hukum Universitas Hasanuddin Makassar.

Adam Josianto Adam, (2014). *Tindak Pidana Cyber Terrorism dalam Transaksi Elektronik*, No. 3, Juli- Oktober 2005.

Nugraha Putera Hafidz, (2014). *Analisis Yuridis Rumusan Delik tentang Tindak Pidana Cyber Terrorism Ditinjau Undang-undang Nomor 15 tahun 2003 tentang*

Pemberantasan Tindak Pidana Terorisme dan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Fakultas Hukum Universitas Sebelas Maret Surakarta.

Harahap Shari Amalina Marissa, (2012). *Analisis Penerapan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dalam Tindak Pidana Siber*, Fakultas Hukum Universitas Indonesia Jakarta.

Ufran, (2014). *Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyber terrorism*, No. 4, Oktober 2014.

Natsir Ivan Nanda, (2009). *Kebijakan Kriminal Terhadap Tindak Pidana Cyber Terrorism*, Fakultas Hukum Universitas Diponegoro Semarang.

Ginting Philemon, (2008). *Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana*, Fakultas Hukum Universitas Diponegoro Semarang.

Ari Mahartha dan Made Mahartayasa, (2016). *Pengaturan Tindak Pidana Terorisme Dalam Dunia Maya (Cyber Terrorism) Berdasarkan Hukum Internasional*, No. 6, Oktober 2016.

https://id.wikipedia.org/wiki/Yurisdiksi. Di akses 11 Desember 2014.

https://supriyadicfc.wordpress.com/2015/06/14/penggunaan-teknologi-informasi-dalam-cyber-terrorism. Di akses 14 Juni 2015.

http://bphn.go.id/data/documents/NA%20RUU%20Perubahan%20atas%20UU%20No%2015%20Tahun%202003%20Tentang%20Pemberantasan%20Tindak%20Pidana%20Terorisme.pdf. Di akses November 2011.