KEBIJAKAN ANTISIPATIF HUKUM DALAM PENANGGULANGAN CYBERTERORRISM DI INDONESIA

Radenta Dwi Krispriyoga,Adam Fadhillah Damanik,Ria Rindika Oktaviana

Fakultas Hukum, Universitas

Diponegoro

radentadwi23@gmail.com

Abstrak

Perkembangan teknologi dapat mengakibatkan semakin luasnya jaringan terorisme melalui internet. Dapat diketahui bahwa *Cyber-Terrorism* masuk telah ditetapkan sebagai kejahatan luar biasa. analisis ini merupakan suatu penelitian yang bersifat yuridis normatif. Untuk menghimpun bahan yang diperlukan, maka telah menggunakan metode penelitian kualitatif, yaitu dengan cara mempelajari buku-buku hukum, artikel artikel yang membahas masalah hukum, himpunan peraturan perundang-undangan yang berlaku di Indonesia, serta berbagai sumber tertulis lainnya. Hasil analisis menunjukkan tentang bagaimana tindak pidana*cyber terrorism* sesuai dengan hukum positif yang berlaku di Indonesia serta bagaimana upaya pencegahan sebagai cara untuk menekan kasus *cyber terrorism* yang ada di Indonesia, bahwa perlunya revisi Undang-Undang Terorisme dan Undang-Undang Informasi dan Transaksi Elektronik yang seharusnya membuat secara khusus tentang *cyber terrorism*, serta penguatan pada sistem jaringan agar masyarakat tidak menjadi korban daripada *cyber terrorism* tersebut.

Kata Kunci: Cyber Terrorism, Internet, Kejahatan Luar Biasa

Abstract

Technological developments can lead to a wider network of terrorism via the internet.It can be seen that the incoming Cyber-Terrorism has been designated as an extraordinary crime. This analysis is a normative juridical study. To collect the necessary material, qualitative research methods have been used, namely, by studying legal books, articlesdiscussing legal issues, a collection of laws and regulations in force in Indonesia, as well as various other written sources. The results of the analysis show how the criminal act of cyber terrorism is in accordance with the positive laws that apply in Indonesia and how prevention efforts as a way to suppress cyber terrorism cases in Indonesia, that there is a need to revise the Terrorism Law and the Law on Information and Electronic Transactions that should be making specifically about cyber terrorism, as well as strengthening the network system so thatpeople do not become victims of cyber terrorism.

Keywords: Cyber Terrorism, Internet, Extraordinary Crime

A. Pendahuluan

Permasalahan mengenai terorisme memang sudah tidak asing lagi bagi kita. Sejarah

tersebut sudah ada sejak zaman dahulu kala dimana ditandai dengan kejahatan berupa pembunuhan dan ancaman yang memiliki tujuan tertentu. Hal ini tidak sesuai dengan tujuan bangsa Indonesia yang terdapat dalam UUD 1945 yaitu melindungi segenap bangsa Indonesia,dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut melaksanakan ketertiban dunia, dengan begitu sangat diperlukan untuk melakukan pemberantasan secara bersama, berencana, terstruktur, sehingga hak asasi manusia dalam hal ini dapat dilindungi dan dijunjung tinggi.

Tindakan terorisme dilakukan secara berencana, terorganisir dan berlaku dimana dan untuk siapa saja tergantung tujuan dari pelaku yang akan melakukan tindakan terorisme tersebut. Biasanya, tindakan teror dibagi dua yaitu teror yang berakibat fisik dan/atau teror yang berakibat nonfisik. Teknologi yang semakin berkembang dengan penggunaan internet merupakan penyebab terjadinya suatu berubahnya sistem sosial dan penyebab terjaidinya pertentangan dalam masyarakat diantaranya adalah revolusi dalam ruang masyarakat. Satjipto Raharjo mengatakanbahwa,[1] *Dalam kehidupan manusia banyak alasan yang dapat dikemukakan sebagai penyebabtimbulnya suatu perubahan di dalam masyarakat, tetapi perubahan dalam penerapan hasil- hasil teknologi modern dewasa in banyak disebut sebagai salah satu penyebab bagi terjadinyaperubahan sosial.*

Terorisme pun kini berkembang lebih cepat yang selalu diikuti dengan berkembangnya teknologi, informasi dan komunikasi. Adanya internet yang terbentuk melalui jaringan komputer yang mana dapat saling menghubungkan antar negara dengan basis *internet protocol*[2]. Jaringan internet ini digunakan oleh pelaku terorisme dengan cara berkomunikasi sesamanya untuk mencari pendukung dengan menyebarkan propaganda melalui situs internet.Selain itu juga para pelaku ini melakukan transaksi bisnis dengan internet untuk membiayai kegiatan mereka dan melakukan *cyber crime* lainnya. Selain itu, pemakaian internet yang digunakan oleh teroris tersebut untuk melakukan kejahatan terorisme disebut dengan *cyber terrorism.* Dalam beberapa literatur hukum internasional

[1] Al Wisnubroto,2010, *Strategi Penanggulangan Kejahatan Telematika*, Yogyakarta: Atma Jaya.
[2] Samad A. N, 2014, *Analisis Instrumen Cyber-Terrorism Dalam Kerangka Sistim Hukum Internasional*, Hlm. 3

disebutkan *cyber terrorism* menjadi bagian atau bentuk dari *cyber crime*. Banyak keuntungan yang diperoleh teroris saat melakukan penyerangan (*cyber attack*) lewat internet. Berbeda dengan teror yang menggunakan bom, para teroris harus beradadi tempat kejadian, dengan menggunakan internet para teroris dapat melakukan aksi tanpa harus berada di tempat kejadian.[3] *Cyber teorrism* ini memang lebih murah yaitu dengan menggunakan internet dan keahlian yang ada, maka aksi terorisme tersebut dpat dilakukan dengan cepat.

Kejahatan dunia maya banyak terjadi di Indonesia maupun negara lainnya. Salah satu contohnya adalah aksi terorisme pada bom Bali I dan II. Dalam kejadian ini Imam Samudra yang ketika masih hidup, ia memberikan laporan saat proses penyelidikan. Imam Samudra menjelaskan bahwa internet merupakan alat yang terbaik untuk mencapai misinya, seperti dalam bukunya yang berjudul *Aku Melawan Teroris*. Yaitu untuk menginstruksikan kepada bawahannya untuk mempelajari internet, sehingga terampil seperti *hacker*.[4] *Hacking* adalah memasukan ke dalam sistem komputer dengan mengenalkan virus agar mudah terkena serangan ke jaringan situs internet, awalnya *hacking* ini bertujuan positif yaitu untuk memperbaiki sistem keamanan yang telah dibangun dan memperkuatnya. Namun, dalam perkembangan tersebut disalahgunakan untuk keperluan yang bersifat merugikan.

Pelaku lainnya yaitu Agung Setyadi dan Mohammad Agung Prabowo alias Max Fiderman akhirnya ditangkap karena dalam situs www.anshar.net yang dibuat oleh mereka ini juga merupakan adanya pergeseran modus penggalangan dana pelaku teroris dengan memanfaatkan *carding* dan pemesanan alat terror melalui dunia maya dibanding menunggu kiriman dari orang tau atau merampok.[5] Setelah dilakukan *decrypt* pada laptop pelaku Bom Bali, akhirnya terbukti internet tersebut telah digunakan untuk melakukan konsolidasi dan koordinasi sebagai target antara lain *hacking*, *virus attack*, *DOS attack*, *phreaking* dan *massive attack*.[6] Ancaman *cyber terrorism* sangat memungkinkan dapat menimpa seluruh negara termasuk Indonesia. Dengan melakukan sarana internet untuk melakukan terorisme ini perlu

[3] Ibid. Hlm 5.
[4] Qutub S, *Cyber Terrorism dalam Tinjauan Hukum Islam*, {s.l.:s.n.,s.a.}, Hlm 5
[5] Antaranews, "Indonesia Pertama Kali Bongkar Kasus Cyber Terrorism" https://www.antaranews.com/berita/42142/indonesia-pertama-kali-bongkar-kasus-cyber-terrorism, diakses 14 Mei 2021.
[6] Dikdik M. Arief Mansyur dan Elisatris Gultom. *Cyber Law* Aspek Hukum Teknologi Informasi. Hlm 68-69

diwaspadai karena dapat merusak seperti fasilitas vital milik negara, fasilitas umumdan, selain itu kegiatan *cyber terrorism* yang menggunakan internet bahkan dapat membuat jatuhnya korban yang lebih besar daripada terorisme yang dilakukan dengan konvensional.

Terdapat beberapa rumusan delik seperti Undang-undang Nomor 15 Tahun 2003 tentang Penetapan Pemerintah Pengganti Undang-undang Nomor 1 Tahun 2002 tentang Tindak Pidana Terorisme menjadi Undang-undang dan UU ITE dapat digunakan bagi pelaku *cyber terrorism*. Tetapi undang-undang tersebut dianggap belum mampu untuk menjerat pelaku tindak pidana teroris di dunia maya karena cakupan dan muatan dalam dunia maya yang sangat majemuk dan begitu luas. Penafsiran terhadap rumusan delik yang ada dapat menjadi salah satu tujuan agar perbuatan tindak pidana yang belum dapat diatur di peraturan perundang-undangan dapat dijeratnya dengan rumusan delik yang berhubungan agar tidak melanggar asas legalitas yang ada.

B. Pembahasan

1. Tindak Pidana Terorisme (*Cyber Terrorism*) dalam Hukum Positif di Indonesia.

Maraknya aksi terorisme saat ini menimbulkan ketakutan tersendiri pada masyarakat. Aksi terorisme tersebut membuat masyarakat bertanya-tanya apakah undang-undang saat ini sudah sesuai dengan yang kondisi yang terjadi, ditambah semakin majunya zaman menyebabkan penyebaran terorisme melalui dunia maya semakin mudah terjadi. Kejahatan terorisme di dunia maya ataru disebut dengan *cyberterrorism* adalah suatu bentuk tindakan melawan hukum yang direncanakan oleh seseorang atau kelompok orang dengan motivasi politis untuk mencapai ideologinya, baik secara langsung maupun tidak langsung, dengan cara melakukan serangan, penyusupan, mencuri, ataupun merusak data informasi, sistem komputer, program,komputer, sehingga dapat menimbulkan korban. *Cyber terrorism* mempunyai 2 (dua) karakteristik, yakni *cyber terrorism* sebagai tindakan teror terhadap sistem komputer, jaringan, dan/ atau basis dan informasi yang tersimpan dalam komputer, serta *cyber terrorism* sebagai penggunaan internet oleh para teroris untuk keperluan organisasi dan media teror kepada pemerintah dan masyarakat. Indonesia memiliki pengaturan di bidang *cyber law* dan pengaturan di bidang terorisme. Meskipun *cyber terrorism* merupakan bagian dari bentuk kejahatan *cyber crime* sebagaimana yang telah diuraikan sebelumnya, namun satu hal yang harus dipahami bahwa sesuai dengan pendapat Denning, *cyber terrorism* merupakan

konvergensi dari *cyberspace* dan terorisme. Oleh karena itu, unsur terorisme dalam *cyber terrorism* juga harus diperhatikan karena kejahatan terorisme memiliki motif tersendiri.[7]

Di Indonesia, pengaturan mengenai kejahatan *cyber terrorism* tidak diatur jelas dan tegas dalam Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 tentang pemberantasan tindak pidana terorisme dan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan transaksi elektronik. Kitab Undang-Undang Hukum Pidana (KUHP) maupun peraturan perundang-undangan yang mengatur di bidang terorisme, juga belum mengatur tindakan ini. Hal tersebut mengakibatkan adanya kekosongan hukum yang mengatur mengenai tindak pidana *cyber terrorism* yang dibuktikan melalui analisa ketentuan hukum yang ada dan berlaku di Indonesia. Adapun bentuk-bentuk perbuatan yang termasuk kategori ini antara lain:

a. *Unauthorized access to computer system and service*, yaitu kejahatan menggunakan system komputer melalui jaringan secara tidak benar dan tanpa ijin dari pemilik.
b. *Denial of service attack (DoS)*, yakni menyerang dengan cara memenuhi jaringan dengan permohonan dalam hitungan detik untuk mendapatkan layanan data sehingga mengakibatkan jaringan bekerja terlalu keras, atau mati, atau melambatnya kinerja jaringan.
c. *Cyber sabotage and extortion*, yaitu kejahatan yang dilakukan dengan menggangu, merusak, atau menghancurkan suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet.
d. *Viruses*, yakni kejahatan yang dilakukan dengan menyebarkan perangkat lunak seperti program, script, atau macro yang telah dirancang untuk menginfeksi, menghancurkan, memodifikasi, dan menimbulkan masalah terhadap komputer atau program komputer.
e. *Physical attacks*, yakni penyerangan fisik yang dilakukan terhadap sistem komputer atau jaringan komputer, dengan cara-cara pembakaran, pencabutan salah satu device komputer atau jaringan yang menyebabkan lumpuhnya sistem komputer.

Beberapa dari kelima perbuatan di atas, jika dikaji merupakan bagian dari perbuatan-perbuatan yang dilarang dalam UU ITE, pada pasal 30 UU ITE, Pasal 32 dan 33 UU ITE.Sama halnya dengan Pasal 30 UU ITE, Pasal 32 UU ITE juga memiliki dua corak sifat melawan hukum. Sifat melawan hukum dalam Pasal 33 UU ITE terletak pada akibat perbuatan tersebut, yakni perbuatan pelaku tersebut akan mengakibatkan terganggunya atau tidak bekerjanya

[7] Zephirinus Jondong, 2020, "Kebijakan Hukum Pidana Bagi Tindak Pidana Cyber Terrorism Dalam Rangka Pembentukan Hukum Positif Di Indonesia," September, Hlm 22-24

sistem elektronik tersebut sebagaimana mestinya. Pasal 30, Pasal 32, dan Pasal 33 UU ITE pada dasarnya ditargetkan untuk mempidana pelaku terorisme *cyber*.

Sebagai catatan, dalam perkembangannya, muncul dua istilah yang semakin sulit untuk dibedakan, yakni munculnya istilah *cyber terrorism* dan terorisme siber (pelaku *cyber crime*) Relevansi Pasal 30, Pasal 32, dan Pasal 33 UU ITE dengan perbuatan tindak pidana cyber terrorism adalah bentuk perbuatan akses tidak sah atau gangguan terhadap data komputer, informasi/ dokumen elektronik milik orang lain atau milik publik yang dilakukan dengan cara pembobolan, penerobosan, dan penjebolan yang melanggar, melampaui sistem pengamanan, dan sebagainya yang memenuhi unsur cara-cara melakukan teror dalam tindak pidana *cyber terrorism*.

Namun, sifat melawan hukum untuk tindak pidana *cyber terrorism* tidak terpenuhi dalam rumusan pasal-pasal UU ITE karena dalam tindak pidana cyber terrorism serangan atau ancaman, secara melawan hukum tersebut dilakukan terhadap komputer, jaringan komputer, dan data yang tersimpan dalam jaringan tersebut, yang memiliki tujuan untuk mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik atau sosial tertentu. Sebagaimana terorisme yang dilakukan secara konvensional yang mengakibatkan kerusakan umum atau suasana teror atau rasa takut terhadap orang secara meluas.

Sama halnya dengan unsur akibat serangan dalam terorisme konvensional, bahwa suatu tindakan dapat dikategorikan sebagai *cyber terrorism* apabila serangan tersebut menciptakan ketakutan dan mengakibatkan korban pada daerah sekitarnya atau secara meluas, meskipun bukan target utama dari serangan mereka. Hal tersebut menjadikan kekosongan hukum dalam pengaturan UU ITE untuk menanggulangi tindak pidana *cyber terrorism*. *Cyber terrorism* tidak diatur dalam berbagai Peraturan Perundang-Undangan di Indonesia. Unsur melawan hukum dalam pengertian tersebut dilakukan dengan perbuatan sepertiancaman atau serangan terhadap komputer, jaringan komputer, dan data yang tersimpan dalamjaringan tersebut, sehingga akibat dari melawan hukum ini menciptakan ketakutan atau merusak infrastruktur dan kehidupan manusia. Dalam situasi seperti ini, pelaku tindak pidana *cyber terrorism* dapat dinyatakan bebas dari pidana karena tidak terdapat unsur melawan hukum yang diatur dalam Undang-Undang melekat pada perbuatannya tersebut. Oleh karena itu, untuk dapat dijatuhi suatu pidana, maka tindak pidana cyber terrorism harus dirumuskan secara jelas dalam Undang-Undang.

2. Upaya pencegahan tindak cyber terorrism yang ada di Indonesia

Upaya pertama yang dapat dilakukan adalah perlunya Badan Nasional Penanggulangan Terorisme untuk melakukan peningkatan sistem jaringan yang mana bisa mendeteksi adanya web atau situs yang terindikasi terorisme dunia maya. Sebab akan cepat tersebar secara luas, apabila tidak secara langsung ditangani, maka akan berdampak dengan pola pikir masyarakat yang dapat berubah. Pemerintah juga sebaiknya apabila merasa adanya ancaman terhadap keamanan nasional pada jaringan, maka seharusnya lansgung memblokir situs tersebut yang terindikasi radikal. Dari beberapa informasi yang kami baca dan telusuri, ternyata mengenai kejahatan komputer ini tidak ada satupun jaringan yang dapat diindikasikan 100% aman dari serangan virus komputer, *spam*, serta *hackers* dan *cyber terrorism*. Karena seorang *hacker* atau *cyber terrorist* yang sudah berpengalaman dapat dengan mudah untuk memasuki sistem jaringan komputer yang menjadi targetnya dengan tidak beralasan bahwa jaringan tersebut sudah memiliki sistem pengamannya atau belum.

Selanjutanya, perlunya revisi undang-undang agar dapat membahas secara rinci mengenai *cyber terrorism*, memang seperti Undang-Undang Nomor 5 Tahun 2018 Tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang dan Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ini dapat digunakan 21 sebatas pasal-pasal yang dapat mendukung atau cocok satu sama lain. Misalnya saja dalam pasal 13 A Undang-Undang Nomor 5 Tahun 2018 yang berbunyi bahwa “Setiap Orang yang memiliki hubungan dengan organisasi Terorisme dan dengan sengaja menyebarkan ucapan, sikap atau perilaku, tulisan, atau tampilan dengan tujuan untuk menghasut orang atau kelompok orang untuk melakukan Kekerasan atau Ancaman Kekerasan yang dapat mengakibatkan Tindak Pidana Terorisme dipidana dengan pidana penjara paling lama 5 (lima) tahun.” Dapat diketahui bahwa meskipun tidak menyebutkan secara khusus menggunakan media internet sebagai media yang digunakan untuk menyebarkan terorisme, namun pasal ini dapat mendekati tindak pidana *cyber terrorism*.

Akan tetapi tetap memiliki kelemahan seperti tidak memberikan definisi secara khusus mengenai *cyber terorrism*, juga tidak selalu para hakim dapat menafsirkan kasus tersebut karena permasalahan *cyber terrorism* yang sangat kompleks. Sehingga, sangat diharapkan

untuk dilakukannya revisi dan dibahas secara khusus mengenai *cyber terorrism*. Perlu diketahui bahwa untuk melakukan pembuktian bahwa seseorang atau kelompok tertentu melakukan tindak pidana *cyber terrorism*, maka dapat melihat beberapa ketentuan yang terdapat pada Undang-Undang Patriot Amerika Serikat yang dapat menjadi pembanding. Namun dapat dijadikan acuan untuk merevisi Undang Undang terorisme dan UU ITE yang memang dalam kejahatan ini telah berkembang menggunakan alat teknologi dan perilaku kejahatannya telah berubah pola dengan menyalahgunakan alat komunikasi dan informasi tersebut.

3. Sanksi Pidana

Mengenai sanksi pidananya juga diharapkan dapat memperhatikan syarat seperti tidak boleh lebih rendah dari ketetapan yang tercantum dalam Undang-Undang sebelumnya, serta mempertimbangkan agar tidak terjadi tumpang tindih produk hukum atau inkonsistensi hukuman.

C. Penutup

Berdasarkan pembahasan yang telah di kemukakan sebelumnya, maka dapat dirumuskan beberapa kesimpulan. Yang pertama *cyber terrorism* merupakan sebuah kejahatan serta ancaman yang baru. *Cyberterrorism* merupakan bentuk transformasi terror yang dilakukan oleh teroris dengan menjadikan jaringan internet sebagai alat atau sasaran serangan. Pelakunyabisa 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*.

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*.

D. Daftar Pustaka

Antaranews.“Indonesia Pertama Kali Bongkar Kasus Cyber Terrorism” https://www.antaranews.com/berita/42142/indonesia-pertama-kali-bongkar-kasus-cyber-terrorism diakses 14 Mei 2021

Mansyur, Dikdik M. Arief dan Elisatris Gultom. Cyber Law Aspek Hukum Teknologi Informasi. Hlm. 68-69.

Qutub S. 2015.Cyber Terorism dalam Tinjauan Hukum Islam. Jakarta: A-Empat

Samad, A. N. (2014). “Analisis Instrumen Cyber-Terrorism Dalam Kerangka Sistim Hukum Internasional”. *Jurnal Lex Crimen* 7.

Wisnubroto, A. (2010). “Strategi Penanggulangan Kejahatan Telematika”. Universitas Atma Jaya Yogyakarta.

Zephirinus, Jondong, 2020, “Kebijakan Hukum Pidana Bagi Tindak Pidana Cyber Terrorism Dalam Rangka Pembentukan Hukum Positif Di Indonesia,” September 2020, Hlm 22-24