



**REKONSEPTUALISASI UPAYA PENANGGULANGAN TINDAK PIDANA
CYBER- TERRORISM DI INDONESIA MELALUI PENDEKATAN
KERAS (HARD APPROACH)**

Muhammad Sulfihan, Nina Lathifa Azalia, Safiyah Inas Shafa

Fakultas Hukum, Universitas Diponegoro

muhammadsulfihan1995@gmail.com

Abstrak

Terorisme tidak lagi hanya dilakukan dengan pelatihan militer. Diera serba canggih saat ini, terorisme juga dapat terjadi melalui media digital atau yang dikenal dengan istilah *cyber terrorism*. *Cyber terrorism* dilakukan dengan memberikan propaganda melalui media online, isi propaganda tersebut berupa kritikan terhadap kinerja pemerintah yang dinilai tidak sejalan dengan tujuan mereka. Selain itu, *cyber terrorism* dapat berupa doktrin yang bisa mempengaruhi pikiran seseorang, akibatnya seseorang terpengaruh dengan ideologi sesat mereka. Metode penelitian dalam karya tulis ilmiah ini adalah yuridis normatif. Oleh karena itu, melalui kebijakan pendekatan keras menjadi langkah preventif sekaligus represif pemerintah dalam penanggulangan *cyber terrorism*.

Kata kunci: *Cyber terrorism, kebijakan hard approach, terorisme*

Abstract

As information and communication technology developed, terrorism was no longer limited to military training. Rather, in today's age of sophistication, terrorism can also occur through digital media or known as cyber terrorism. Cyber terrorism is countered by providing propaganda through online media, the content of it is a criticism of government performance that is judged to be incompatible with their goals. In addition cyber terrorism can be a doctrine that can affect one's mind, causing the individual to be affected by their misguided ideologies. The method of research in this scientific literature is normative juridical legal research. Thus, through hard approach policy becomes a government's preventive and repressive measure in the counter terrorism.

Keywords: *Cyber terrorism, hard approach policy, terrorism*

A. Pendahuluan

Terorisme bukan hal baru di dunia, namun, seiring perkembangan zaman maka terorisme pun ikut berkembang, yaitu menjadi *cyber terrorism*. Pengguna *smartphone* di dunia saat ini mencapai 5,22 miliar orang, dengan jumlah pengguna internet mencapai 4,66 miliar orang¹. Di Indonesia, jumlah pengguna internet hingga tahun 2021 mencapai 202 juta jiwa.

¹ Agustin Setyo Wardani, "Pengguna Internet Dunia Tembus 4,66 Miliar, Rata-Rata Online Di Smartphone," *Liputan6*, January 28, 2021, <https://m.liputan6.com/tekno/read/4469008/pengguna-internet-dunia-tembus-466-miliar-rata-rata-online-di-smartphone>.



Definisi *cyber terrorism* dikemukakan oleh James A. Lewis yang mendefinisikan *cyber terrorism* sebagai penggunaan perangkat jaringan komputer untuk mematikan infrastruktur nasional yang cukup penting (energi, transportasi, dan berjalannya pemerintahan) atau untuk mengganggu atau mengintimidasi sebuah pemerintahan atau kelompok warga negara (*civilian population*)². *Cyber terrorism* pada dasarnya bertujuan untuk melakukan penyerangan terhadap objek vital pemerintah maupun kebijakan pemerintah yang terhubung dengan internet yang tidak sejalan dengan tujuan ideologi yang mereka pegang. Salah satu modus yang teroris lakukan adalah dengan menyebarkan propaganda. Menurut Rahmani Dayan, terdapat karakteristik khusus yang dimiliki terorisme namun tidak dimiliki oleh kejahatan-kejahatanlain yaitu tindakan tersebut dilakukan secara terstruktur, melebar, dan terorganisir sehingga menjadi ancaman yang sangat serius bagi masyarakat, bangsa, dan negara. Maka dari itu, *cyber terrorism* termasuk kategori “*Transnational Organize Crime*”³.

Luasnya cakupan dan efeknya yang sangat besar ini membuat hukum nasional tidak akan cukup untuk menanggulangi tindak pidana *cyber terrorism* karena hukum nasional belum secara tegas mengatur mengenai tindak pidana ini. Melihat kurang optimalnya penanganan tindak pidana *cyber terrorism* maka diperlukan regulasi dan kebijakan yang dapat menghentikan sepaik terjang penyebaran propaganda oleh teroris melalui media digital dengan menggunakan kebijakan yang bersifat pendekatan keras (*hard approach*).

B. Pembahasan

1. Kebijakan Pemerintah dalam Mengurangi Kecemasan Masyarakat Akan *Cyber Terrorism*

Cyber terrorism adalah tindakan kriminal yang dilakukan melalui komputer dan berakibat kejahatan, kematian dan/atau kehancuran, dan menimbulkan teror untuk tujuan memaksa pemerintah untuk mengubah kebijakan mereka⁴. Tujuan utama dari *cyber*

² Ufran, “Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism - Neliti” 43, no. 4 (2014), <https://www.neliti.com/id/publications/158219/kebijakan-antisipatif-hukum-pidana-untuk-penanggulangan-cyberterrorism>.

³ Oki Putri Andini, “TINJAUAN YURIDIS TINDAK PIDANA CYBER TERRORISM DALAM PERSPEKTIF KEJAHATAN TRANSNASIONAL TERORGANISIR,” <http://lib.unnes.ac.id/39108/>.

⁴ Alfira Nurliliani Samad, 2014, “SKRIPSI ANALISIS INSTRUMEN CYBER-TERRORISM DALAM KERANGKA SISTEM HUKUM INTERNASIONAL OLEH : ALFIRA NURLILIANI SAMAD”.

<https://docplayer.info/30171025-Skripsi-analisis-instrumen-cyber-terrorism-dalam-kerangka-sistim-hukum-internasional-oleh-alfira-nurliliani-samad-b.html>.



terrorism ialah memberikan teror serta memaksa pemerintah mengubah kebijakan mereka jika tidak sesuai dengan tujuan ideologi para teroris tersebut. Target utama *cyberterrorism* merupakan pemerintah, masyarakat sipil, dan juga sistem komputer. Selain menargetkan infrastruktur yang berbasis pada teknologi komunikasi dan informasi, masyarakat sipil memang menjadi target yang paling mudah ditembus oleh *cyber terrorism*. Salah satu kasus yang paling besar adalah kasus *cyber terrorism* di Srilanka tahun 1988. Kasus tersebut dilakukan oleh organisasi teroris Geurilla, mereka mengirimkan email pada Kedutaan Sri Lanka sebanyak 800 email perhari dan hal tersebut terjadi selama dua minggu. Di Indonesia, *cyber terrorism* pernah terjadi pada tahun 2017 di mana teroris menyerang rumah sakit di Indonesia dan dunia dengan serangan *ransomewareWannacry*. Program itu menyadara sistem sejumlah rumah sakit sehingga menyulitkan pelayanan medis untuk pasien.⁵

Regulasi hukum mengenai terorisme sendiri telah diatur dalam Undang-Undang Republik Indonesia 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. Pasal 1 undang-undang tersebut menjelaskan jika terorisme merupakan perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan teror atau rasa takut yang menimbulkan korban yang bersifat massal, dan/atau menimbulkan kerusakan terhadap objek vital yang strategis dengan motif ideologi, politik, atau gangguan keamanan⁶. Namun, pada undang-undang ini belum mengatur secara spesifik mengenai *cyber terrorism*.

Namun sekarang Indonesia sudah memiliki Undang-Undang Nomor 11 Tahun 2008 tentang ITE yang dapat mengatur tingkah laku para pengguna internet agar tidak berbuat sewenang-wenang di dunia maya. Beberapa pasal pada kedua undang-undang tersebut dapat digunakan untuk menjerat tindak pidana *cyber terrorism*, walaupun ada beberapa pasal yang juga tidak sinkron jika digabungkan. Maka untuk menghukum pelaku *cyber terrorism* dapat *men-jucto* beberapa pasal dalam kedua undang-undang tersebut.

⁵ Oik Yusuf, "Rumah Sakit Indonesia Jadi Korban 'Terorisme Cyber' Halaman All - Kompas.Com," <https://tekno.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber.?page=all>.

⁶ Indonesia. Undang-Undang Republik Indonesia 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. UU No. 5 Tahun 2018. LN. No. 92 Tahun 2018, TLN. 6216.



Hukum positif di Indonesia sebenarnya masih sangat lemah untuk menjerat pelaku tindak pidana *cyber terrorism* karena peraturan perundang-undangan yang mengatur tindak pidana tersebut yaitu Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 dan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 belum menjelaskan secara merinci mengenai tindak pidana ini. Peraturan tersebut tidak secara jelas menyebutkan tindak pidana *cyber terrorism* sehingga menimbulkan ketidakpastian hukum dan kekosongan hukum⁷. Maka dari itu untuk mengatasi kecemasan serta ketakutan yang dialami masyarakat, pemerintah Indonesia menerapkan kebijakna yang lebih konkrit yaitu kebijakan dengan pendekatan keras (*hard approach*), di mana kebijakan tersebut dilakukan dengan pengontrolan penggunaan internet dalam bentuk penutupan situs tertentu yang dianggap radikal, penyaringan *IP address*, hingga penyaringan pada mesin pencari.

2. Konsep Kebijakna dengan Pendekatan Keras (*Hard Approach*)

Hard approach merupakan suatu pendekatan yang memerlukan kekerasan berupa aksi militer untuk menyelesaikan sebuah permasalahan yang timbul dari berbagai pihak. Contoh tindakan dengan melakukan pendekatan keras, seperti membunuh, menangkap atau menahan, menggunakan senjata tajam, dan masih banyak lagi agar pelaku teroris berhenti melakukan aksinya. Konsep pendekatan keras (*hard approach*) dapat dilakukan dengan operasi militer untuk menjaga keamanan di seluruh wilayah negara dari para terorisme. Selain itu, pasukan militer harus selalu siap untuk menghadapi serangan dari para teroris yang mengancam keamanan dan ketertiban negara.

Dampak negatif penggunaan internet membawa sifat malas pada anak atau remaja dan lebih parahnya lagi media internet dijadikan oleh para teroris atau oknum tidak bertanggung jawab untuk mengganggu pengguna hingga si pengguna terkena gangguan mental yang menyebabkan korban melakukan bunuh diri. Selain itu, jejak digital yang telah tersebar di seluruh media sosial juga mengakibatkan ketidaknyamanan seseorang ketika melakukan aktivitas di dunia internet. Sehingga pemerintah melakukan berbagai cara agar hak asasi manusia maupun kenyamanan warga negara terjaga. Upaya yang dilakukan pemerintah untuk menanggulangi kejahatan terorisme melalui konsep pendekatan *hard approach* dirasa sangat

⁷ Agis Josianto Adam, 2014, "TINDAK PIDANA CYBER TERRORISM DALAM TRANSAKSI ELEKTRONIK", *LEX ADMINISTRATUM*," Vol. 2, No. 3.
<https://ejournal.unsrat.ac.id/index.php/administratum/article/view/6145>.



Al-Hakam Islamic Law & Contemporary Issues, Volume 2 Edisi 2 October 2021
diperlukan mengingat kejahatan terorisme ini merupakan kejahatan luar biasa yang dapat mengganggu keamanan dan ketertiban negara.

C. Penutup

Berdasarkan uraian di atas, dapat disimpulkan beberapa kesimpulan. Yang pertama, perbuatan *cyber terrorism* menyebar teror dan ketakutan melalui perantara komputer dengan sasaran yang dituju seperti masyarakat sipil maupun pemerintah. Untuk menanggulangi hal tersebut, pemerintah menetapkan regulasi hukum melalui UU No 5 Tahun 2018 Tentang Perubahan Atas UU No 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang No 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme dan melalui UU No 5 Tahun 2018 jo UU No 11 Tahun 2008. Yang kedua, dengan berkembangnya teknologi dapat mempermudah berbagai urusan manusia.

Selain itu terdapat saran berupa kebijakan dengan pendekatan keras (*hard approach*) dalam memutus rantai kejahatan siber khususnya *cyber terrorism*.

D. Daftar Pustaka

- Adam, Agis Josianto. 2014. "TINDAK PIDANA CYBER TERRORISM DALAM TRANSAKSI ELEKTRONIK", *LEX ADMINISTRATUM*. Vol.2. No. 3. <https://ejournal.unsrat.ac.id/index.php/administratum/article/view/6145>.
- Andini, Oki Putri. "TINJAUAN YURIDIS TINDAK PIDANA CYBER TERRORISM DALAM PERSPEKTIF KEJAHATAN TRANSNASIONAL TERORGANISIR," <http://lib.unnes.ac.id/39108/>.
- Indonesia. Undang-Undang Republik Indonesia 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. UU No. 5 Tahun 2018. LN. No. 92 Tahun 2018, TLN. 6216.
- Samad, Alfira Nurliliani. "SKRIPSI ANALISIS INSTRUMEN CYBER-TERRORISM DALAM KERANGKA SISTIM HUKUM INTERNASIONAL OLEH: ALFIRA NURLILIANI SAMAD B - PDF Download Gratis," <https://docplayer.info/30171025-Skrripsi-analisis-instrumen-cyber-terrorism-dalam-kerangka-sistim-hukum-internasional-oleh-alfira-nurliliani-samad-b.html>.
- Ufran. 2014 "Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism - Al-Hakam Islamic Law & Contemporary Issues. Volume 2 Edisi 2 October 2021



Al-Hakam Islamic Law & Contemporary Issues, Volume 2 Edisi 2 October 2021
Neliti” 43, No. 4 <https://www.neliti.com/id/publications/158219/kebijakan-antisipatif-hukum-pidana-untuk-penanggulangan-cyberterrorism>.

Wardani, Agustin Setyo. “Pegguna Internet Dunia Tembus 4,66 Miliar, Rata-Rata Online Di Smartphone.” *Liputan6*. <https://m.liputan6.com/teknoread/4469008/pegguna-internet-dunia-tembus-466-miliar-rata-rata-online-di-smartphone>.

Yusuf, Oik. “Rumah Sakit Indonesia Jadi Korban ‘Terorisme Cyber’ Halaman All - Kompas.Com,”
<https://teknoread.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber.?page=all>.