Kebijakan Hukum Pidana Terhadap Upaya Pemberantasan Terorisme Siber Di Indonesia

Danang Enggartyasto dan Irwan Hafid
Magister Hukum Fakultas Hukum Universitas Islam Indonesia Yogyakarta Indonesia
Jln. Kaliurang Km. 14,5 Sleman Yogyakarta Indonesia
enggarjob@gmail.com; irwan.hafidz@gmail.com

Abstract

Cyber terrorism is a type of cyber crime that arises as a result of the negative impact of the development of technology and information. These actions arise due to changes in people's behaviorial patterns that are leaning towards computer abuse. The motivation for the crime of cyber terrorism is for the benefit of certain groups with the aim of showing their existence on the world political stage. This research is juridical normative, which is carried out by reviewing or analyzing secondary data in the form of legal materials, especially primary legal materials, secondary legal materials, and tertiary legal materials. The results of this study conclude that the current regulation of cyber terrorism is not comprehensive enough to mitigate cyber terrorism. Hence in the future, a criminal law policy, both penal and non-penal, is needed in eradicating cyber-terrorism crimes more optimally.

Key Words: Policy; criminal; terrorism; cyber

Abstrak

Terorisme siber merupakan salah satu jenis tindak pidana dunia maya yang muncul akibat dari dampak negatif perkembangan teknologi dan informasi. Tindakan tersebut muncul akibat perubahan pola perilaku masyarakat terhadap penyalahgunaan komputer. Motivasi dari aksi kejahatan terorisme siber adalah untuk kepentingan kelompok tertentu dengan tujuan untuk menunjukkan eksistensinya dipanggung politik dunia. Penelitian ini bersifat yuridis normatif, yakni dilakukan dengan cara mengkaji atau menganalisis data sekunder yang berupa bahan hukum terutama bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Hasil penelitian ini menyimpulkan bahwa pengaturan tindak pidana terorisme siber yang ada saat ini belum cukup komprehensif dalam mengatur terorisme siber. Sehingga ke depan diperlukan kebijakan hukum pidana, baik secara penal dan non-penal dalam menanggulangi tindak pidana terorisme siber agar lebih optimal..

Kata-kata Kunci: Kebijakan; pidana; terorisme; siber

Pendahuluan

Penelitian ini dilatarbelakangi oleh empat permasalahan dasar. *Pertama,* pesatnya perkembangan teknologi dan informasi dapat membawa suatu perubahan besar dalam kehidupan sosial budaya masyarakat secara global.[1] Teknologi mampu mengembangkan ruang gerak kehidupan baru bagi masyarakat. Tanpa disadari komunitas manusia dapat bergerak dalam dua kehidupan sekaligus, yakni kehidupan masyarakat nyata dan kehidupan masyarakat maya *(cyber community).*[2] Bahkan dengan teknologi, dunia menjadi tanpa batas *(borderless)* dan menyebabkan pergeseran perilaku masyarakat secara sosial dengan begitu cepat.[3] Sekarang masyarakat tidak lagi dihalangi oleh batas-batas teritorial suatu negara yang dahulu ditetapkan sangat esensial sekali.

Kedua, perkembangan teknologi dan informasi ibarat pedang bermata dua, selain memberi kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, perkembangan teknologi juga menjadi sarana efektif dalam melakukan kejahatan atau perbuatan melawan hukum.[4] Dampak negatif dari perubahan pola perilaku pada era kehidupan global tersebut nampak dari berkembangnya kriminalitas baik secara kuantitatif maupun kualitatif. Berbagai jenis kejahatan dengan dimensi baru seperti penyalahgunaan komputer, kejahatan perbankan, hingga kejahatan terorisme siber bermunculan mewarnai perkembangan teknologi.[5]

Ketiga, maraknya kasus terorisme siber secara global maupun spesifik di Indonesia, membuat persoalan terorisme semakin kompleks. Salah satu kasus terorisme siber yang pernah menghebohkan publik ialah munculnya serangan virus *ransomware wannacry* terhadap beberapa rumah sakit di hampir 100 negara

---

[1] Mohammad Ngafifi, "Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya", *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, Vol. 2, No. 1, 2014, hlm. 36

[2] Masyarakat nyata adalah sebuah kehidupan masyarakat yang secara indrawi dapat dirasakan sebagai sebuah kehidupan nyata, dimana hubungan-hubungan sosial sesama anggota masyarakat dibangun melalui pengindraan. Secara nyata kehidupan masyarakat manusia dapat disaksikan sebagaimana apa adanya. Sedangkan kehidupan masyarakat maya adalah sebuah kehidupan masyarakat manusia yang tidak dapat secara langsung diindra melalui (seluruh) pengindraan manusia, namun dapat dirasakan dan disaksikan sebagai sebuah realitas. Realitas kehidupan ini bukanlah dunia akhirat manusia, bukan pula bagian dari dunia metafisika, namun merupakan sisi lain dari kehidupan materi manusia di bumi dan alam jagad raya. Realitas kehidupan ini adalah bagian yang tak terlepaskan dari penciptaan mega-budaya manusia serta budaya kontemporer yang dicapai oleh manusia. Lihat Burhan Bungin, "Cybercommunity, Konstruksi Sosial Teknologi Telematika Atas Realitas Masyarakat Maya", *Pidato Pengukuhan Jabatan Guru Besar dalam Ilmu Sosiologi Komunikasi Pada Universitas 17 Agustus 1945 Surabaya,* 2002, hlm. 14

[3] Agus Raharjo, *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Bandung, Citra Aditya Bahkti, 2002, hlm. 5

[4] Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum di Indonesia*, Bandung, Refika Aditama, 2004, hlm. 1

[5] Aloysius Wisnubroto, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Yogyakarta, Penerbit Universitas Atma Jaya Yogyakarta, 1999, hlm. 1-5

diseluruh dunia, termasuk Indonesia.[6] Munculnya virus tersebut diduga akibat serangan yang menggunakan media internet untuk membuat sistem komputer dan peralatan teknologi rumah sakit lumpuh. Akibatnya pelayanan rumah sakit menjadi berantakan, seperti sulitnya pasien dan dokter mengakses rekam medis karena gangguan komputer.

Keempat, pengaturan terorisme siber di Indonesia saat ini bersifat sektoral, baik dalam Kitab Undang-Undang Hukum Pidana (KUHP), UU No. 11 Tahun 2008 tentang Informasi dan Transasksi Elektronik sebagaimana telah diubah dengan UU No. 19 Tahun 2016 (UU ITE), UU No. 36 Tahun 1999 tentang Telekomunikasi, dan UU No. 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang sebagaimana telah diubah dengan UU No. 5 Tahun 2018 (UU Terorisme). Pengaturan *a quo* lebih bersifat gangguan terhadap ketertiban umum yang dilakukan oleh setiap orang dengan perantara telekomunikasi dan teknologi sehingga tidak terlalu menjangkau aturan secara spesifik tindakan teroris yang memanfaatkan teknologi dalam aksinya.

Rumusan Masalah

Berangkat dari latar belakang masalah di atas, maka rumusan masalah dalam penelitian ini adalah: *Pertama*, bagaimana pengaturan hukum pidana terhadap pemberantasan tindak pidana terorisme siber di Indonesia saat ini? *Kedua*, bagaimana upaya kebijakan hukum pidana yang dapat dibangun dalam upaya pemberantasan tindak pidana terorisme siber di Indonesia ke depan?

Tujuan Penelitian

Adapun tujuan penelitian ini yaitu: *Pertama,* untuk mengetahui pengaturan hukum pidana terhadap pemberantasan tindak pidana terorisme siber di Indonesia saat ini. *Kedua,* untuk mengetahui dan menganalisis bentuk kebijakan hukum pidana terhadap upaya pemberantasan tindak pidana terorisme siber di Indonesia ke depan.

Metode Penelitian

Penelitian ini merupakan penelitian hukum normatif yang mengkaji pengaturan serta bentuk kebijakan hukum pidana terhadap tindak pidana

[6] Oik Yusuf, "Rumah Sakit Indonesia jadi Korban Terorisme *Cyber*" dalam *https://tekno.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber.?page=all,* diakses pada 28 Oktober 2021

terorisme siber di Indonesia. Bahan hukum yang digunakan adalah bahan hukum primer, bahan hukum sekunder, serta bahan hukum tersier. Sementara pendekatan yang digunakan ialah pendekatan perundang-undangan (*statute approach*) dan pendekatan konsep (*conseptual approach*). Bahan hukum dikumpulkan dengan dua cara, yakni studi dokumen dan studi literatur yang terkait dengan pengaturan terorisme siber. Setelah itu, temuan hasil penelitian yang diperoleh dari ketiga bahan hukum di atas, selanjutnya dianalisis secara deskriptif kualitatif melalui tiga alur kegiatan, yakni reduksi bahan hukum, penyajian bahan hukum, serta penarikan kesimpulan.

Hasil Penelitian dan Pembahasan

Pengaturan Terorisme Siber di Indonesia

Secara umum terorisme dimaknai sebagai serangan terkoordinasi yang bertujuan membangkitkan perasaan teror terhadap sekelompok masyarakat.[7] Namun demikian, definisi terkait terorisme hingga saat ini masih terus mengalami perdebatan meskipun sudah dirumuskan oleh para ahli atau telah didefinisikan dalam peraturan perundang-undangan. Ketiadaan definisi yang seragam menurut hukum internasional membuat setiap negara mendefinisikannya menurut sistem hukum masing-masing negara.

Terorisme siber merupakan salah satu dimensi baru dari kejahatan masa kini (secara umum) atau transformasi dari terorisme konvensial (secara khusus). Isitilah terorisme siber *(cyber terrorism)* ini muncul dalam pemberitaan media dengan istilah yang berbeda-beda. Tidak adanya istilah baku yang digunakan untuk mendefinisikan tindak pidana terorisme dan terorisme siber menyebabkan kesulitan secara teoritis dan konseptual. Dari kedua istilah itu, terdapat persamaan bahwa sama-sama ditujukan untuk kegiatan ancaman terorisme, sementara perbedaan mendasar terletak pada penggunaan teknologi (terorisme siber) dan terorisme konvensional seperti bom bunuh diri dalam menjalankan aksinya.

Terorisme siber atau *cyber terrorism* merupakan salah satu jenis kejahatan yang termasuk dalam *cyber crime,* meliputi *cyber pornography*, *cyber harassment*, dan *cyber stalking crimes.*[8] *Cyber-terrorism* merupakan konvergensi terorisme dan *cyberspace.*[9] Terorisme siber merupakan serangan teroris yang menggunakan

---

[7] Indriyanto S. Adji, *Terorisme dan HAM dalam Terorisme: Tragedi Umat Manusia,* Jakarta, O.C. Kaligis & Associates, 2001, hlm. 17

[8] Eka L. Marpaung, Mila Astuti, dan Ali Ibrahim, "Analisis *Cyber Law* dalam Pemberantasan *Cyber Terrorism* di Indonesia", *Prosiding Annual Research Seminar Computer Science and ICT,* Vol. 3, No. 1, 2017, hlm. 18

[9] Eska N. Sarinastiti dan Nabila K. Vardhani, "Internet dan Terorisme: Menguatnya Aksi Global *Cyber Terrorism* Melalui New Media", *Jurnal Gama Societa,* Vol. 1, No. 1, 2018, hlm. 43

peralatan jaringan komputer *(cyberspace)* untuk mengganggu sistem infrastruktur negara (energi, transportasi, operasional pemerintahan, dan sejenisnya) atau untuk mengintimidasi pemerintahan atau sekelompok masyarakat sipil.[10] *Cyberspace* merupakan metode pengiriman pesan yang menarik untuk teroris. Akses dengan *cyberspace* lebih mudah diperoleh dibandingkan media konvensional. Hanya melalui internet, teroris bisa melaksanakan aksinya dari jarak jauh, bahkan beda negara.

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.* Indonesia telah meratifikasi konvensi tersebut 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*.[11]

Meskipun belum memuat secara khusus aturan mengenai *cyber terrorism*, terminologi *cyber terrorism* mulai dipergunakan dalam *ASEAN Convention on Counter Terrorism.* 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.[12] 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 hukum, yakni 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.[13]

---

[10] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", dalam *https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_ files/files/media/csis/pubs/021 101_risks_of_cyberterror.pdf,* diakses pada 29 Oktober 2021

[11] Alfira N. Samad, *Analisis Instrumen Cyber Terrorism dalam Kerangka Sistem Hukum Internasional*, Makassar, Universitas Hasanuddin, 2014, hlm. 4

[12] Article VI, ASEAN Convention on Counter Terrorism: *"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. Lihat* Ari Mahartha dan Made Mahartayasa, "Pengaturan Tindak Pidana Terorisme dalam Dunia Maya *(Cyber Terrorism)* Berdasarkan Hukum Internasional, *Jurnal Kertha Negara,* Vol. 4, No. 6, 2016, hlm. 4

[13] *Ibid*

Harmonisasi pengaturan hukum mengenai *cyber terrorism* sangat 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.[14]

Dalam konteks itu, pengaturan yang relatif terkait untuk menjerat pelaku terorisme siber di Indonesia saat ini ialah: *Pertama,* ketentuan dalam KUHP. Perumusan tindak pidana dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan terorisme siber yang merupakan bagian dari *cyber crime.* Di samping itu, KUHP juga mengandung berbagai kelemahan dan keterbatasan dalam mengahadapi perkembangan teknologi dan *high tech crime* yang sangat bervariasi. Meskipun demikian, beberapa pasal KUHP yang dapat digunakan untuk menjerat tindak pidana terorisme siber salah satunya ialah kejahatan terhadap ketertiban umum (Bab V), Pasal 168 ayat (1), (2), dan (3), kejahatan terhadap nyawa (Bab XIX), Pasal 340, pencurian (Bab XXII) Pasal 362, serta pemerasan dan pengancaman (Bab XXIII), Pasal 368.

Berkaitan dengan permasalahan tersebut, jika KUHP ingin digunakan untuk menanggulangi tindak pidana terorisme siber haruslah diperhatikan terlebih dahulu batasan ruang lingkup, unsur, dan bentuknya, sehingga dapat dikatakan sebagai *cyber terrorism.* Unsur-unsur tersebut antara lain:[15] (i) serangannya melalui dunia maya, bermotivasi politik, dan mengarah pada kematian luka-luka; (ii) menyebabkan ketakutan atau merugikan secara fisik atas serangan dari dunia maya tersebut; (iii) serangannya serius untuk melawan atau ditujukan ke infrastruktur informasi vital seperti keuangan, energi, transportasi dan pemerintahan; (iv) serangan yang mengganggu sarana yang tidak penting, bukan dikategorikan sebagai aksi *cyber terrorism*; serta (v) serangan itu tidaklah semata-mata dipusatkan pada keuntungan moneter.

Kedua, pengaturan dalam UU ITE. Indonesia telah mengesahkan UU yang berkaitan dengan kejahatan dunia maya (*cybercrime*), yaitu UU ITE. Regulasi tersebut bertujuan untuk mengharmonisasikan antara instrumen peraturan hukum nasional dengan instrumen hukum internasional yang mengatur

[14] *Ibid.,* hlm. 5

[15] Zahri bin Yunos, "Addresing Cyber Terrorism Threats" dalam *https://observatoire-fic.com/en/addressing-cyber-terrorism-threats-by-zahri-bin-yunos-cybe rsecurity-malaisia/*, diakses pada 30 Oktober 2021

teknologi informasi diantaranya, *The United Nations Commissions on International Trade Law*, *World Trade Organization*, *Uni Eropa*, *Asia Pacific Economic Cooperation*, *Association of Southeast Asian Nations*, dan *Organisation for Economic Co-operation and Development*. Masing-masing organisasi mengeluarkan aturan yang dapat mengisi satu sama lain.[16]

Beberapa aturan pasal yang mengandung muatan tindak pidana dalam bidang *cyber crime,* dapat ditemukan dalam Pasal, 28, Pasal 29, Pasal 30, Pasal 31, Pasal 32, Pasal 33, Pasal 34, Pasal 35, Pasal 45, serta Pasal 52 UU ITE. Melihat berbagai ketentuan yang telah dikriminalisasikan dalam UU ITE tersebut, nampak adanya kriminalisasi terhadap perbuatan yang pada umumnya berhubungan dengan penyalahgunaan di bidang teknologi Infomasi dan Transaksi Elektronik, termasuk didalamnya yang berbentuk tindak pidana terorisme siber.

Ketiga, pengaturan dalam UU Telekomunikasi. *Cyber terrorism* sebagai salah satu kejahatan dunia maya yang dilakukan dengan media internet (upaya pemanfaatan alat komunikasi) merupakan salah satu perbuatan berhubungan dengan kepentingan umum, keamanan dan ketertiban umum. Hal tersebut dapat terlihat dari hal-hal yang memungkinkan di lakukannya perbuatan terorisme siber atau penggunaan internet sebagai salah satu sarana telekomunikasi untuk tujuan perbuatan terorisme siber yang dapat mengganggu kepentingan publik, kesusilaan, keamanan dan ketertiban umum, seharusnya juga merupakan tanggung jawab penyelenggara telekomunikasi.

Oleh karenanya, ketentuan pidana sebagaimana diatur dalam undang-undang ini juga bisa digunakan untuk menjerat tindakan terorisme siber. Hal tersebut dapat dilihat dalam Bab VII, yakni dalam Pasal 47, Pasal 50, Pasal 52, Pasal 53, Pasal 55, Pasal 56, Pasal 57, dan Pasal 59. Secara umum, pasal-pasal tersebut hanya mengatur terkait kejahatan dalam bidang telekomunikasi, tetapi tindakan terorisme siber bisa dijerat menggunakan pasal tersebut, karena tindakannya cenderung akan menggunakan media telekomunikasi dalam melancarkan aksinya.

Keempat, pengaturan dalam UU Terorisme. Pada dasarnya, pengaturan mengenai terorisme siber harusnya diatur secara komprehensif dalam UU Terorisme. Namun dalam realitas perundang-undangan di Indonesia, tindak pidana terorisme siber tersebut diatur secara sektoral dalam beberapa undang-undang, seperti KUHP, UU ITE, dan UU Telekomunikasi. Ketiadaan aturan yang rinci mengenai terorisme siber ternyata juga berimplikasi pada peraturan

[16] Barda N. Arief, *Tindak Pidana Mayantara*: *Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta, PT. Raja Grafindo Persada, 2006, hlm. v

perundang-undangan. Dimana pengaturan terorisme siber cenderung lebih sering dijerat UU ITE, dibandingngkan UU Terorisme sendiri.

Hal itu tentu tidak terlepas dari pemahaman bahwa setiap orang yang melakukan kejahatan melalui teknologi sudah dikategorikan sebagai terorisme siber. Menurut Andrew M. Colarik, pelaku terorisme siber ialah teroris yang sesungguhnya sehingga harus diatur dalam UU Terorisme. Jika mengacu pendapat tersebut, maka pengaturan terorisme siber dalam UU Terorisme hanya diatur dalam Pasal 1 angka 4 dan Pasal 12 B ayat (3), selebihnya mengatur terorisme dalam arti umum.

Kasus dan Modus Operandi Terorisme Siber

Kasus terorisme siber telah banyak terjadi di berbagai negara, termasuk di Indonesia. Kasus tersebut diantaranya:[17] (i) Kedutaan Besar Sri Lanka di berbagai negara dibanjiri oleh hampir 800 email yang semua berisi tentang ancaman (1997). Kelompok yang mengancam tersebut menyebut diri mereka sebagai *Black Tigers*; (ii) sekelompok *hacker* China mematikan satelit China (1997); (iii) sabotase internet terjadi di *Babha Atomic Research Centre,* India (1998); (iv) infrastruktur informasi di Estonia diserang oleh gerakan yang menamakan dirinya *Eurasian Youth Movement* (2007); (v) *cyber terrorism* juga terjadi di Eropa, yang dilakukan oleh *Greek Security* and *Intrude.* serangan dilakukan terhadap sistem komputer *European Organization for Nuclear Research* (pengembangan nuklir terbesar di dunia pada 2008); serta (vi) Pada 2016 muncul serangan virus *ransomware wannacry* terhadap beberapa rumah sakit di hampir 100 negara diseluruh dunia, termasuk Indonesia. Munculnya virus tersebut diduga akibat serangan yang menggunakan media internet untuk membuat sistem komputer dan peralatan teknologi rumah sakit lumpuh

Gerakan terorisme siber ini sangat berbahaya dan patut diwaspadai, apalagi kelompok yang menjalankan ialah kelompok teroris. Misalnya saja, pelaku Bom Bali (Imam Samudra) menyatakan bahwa internet adalah alat yang terbaik untuk mencapai misinya. Pernyataan itu ia tuangkan dalam bukunya yang berjudul "Aku Melawan Teroris (*I Fight terorists*)". Ia menyarankan kepada junior-juniornya untuk belajar internet, sehingga terampil seperti *hacker*. Bagi mereka, tujuan utamanya ialah untuk berbagi pengetahuan mengenai *hacking*, serta sebagai alat perlawanan politik.[18]

---

[17] Bayu Widianto, "Dampak Serangan Virtual ISIS *Cyber-Caliphate* Terhadap Amerika Serikat", *International and Diplomacy,* Vol. 2, No. 2, 2017, hlm. 177-178

[18] Marquerite A. Sapiie, "Indonesia Joins World to Fight Cyber Terrorism" dalam *https://www.thejakartapost.com/news/2015/12/10/indonesia-joins-world-fight-cy ber -terrorism.html,* diakses pada 30 Oktober 2021

Untuk memahami bagaimana para pelaku terorisme siber tersebut bekerja, berikut beberapa hal penting yang harus diperhatikan. *Pertama,* pelaku *(actors)* dari terorisme siber sebagian besar merupakan teroris. Andrew Michael Colarik menegaskan bahwa, *"there is no cyber terrorism without terrorism"*.[19] Pernyataan tersebut menegaskan bahwa pelaku *cyber terrorism* merupakan para teroris. Mereka melancarkan kegiatan terornya dengan menggunakan fasilitas siber. Penggunaan komputer sebagai alat dan sasaran serangan merupakan bentuk penggunaan kekerasan dan intimidasi, khususnya untuk tujuan politik tertentu.[20]

Kedua, alat *(tools)* yang digunakan ialah dengan memanfaatkan jaringan komputer. Pelaku atau kelompok pelaku melakukan serangan secara masif untuk melakukan penetrasi terhadap jaringan keamanan komputer (menghilangkan atau mematikan fungsi pentingnya). Adapun sasaran utamanya ialah infrastruktur penting, seperti *public health, emergency services, government, defense industrial base, information and tellecomunication, banking and finance, transportation, etc.*[21]

Ketiga, menurut Phillip W. Brunst, ada beberapa motivasi umum kenapa kejahatan dilakukan di internet. Beberapa faktor-faktor yang menjadi motivasi, yaitu: *location independence*, *speed, anonymity, internationality, dan cost-benefit ratio.*[22] Lebih lanjut Brunst menjelaskan lima bentuk motivasi tersebut berlaku bagi kejahatan *cyber terrorism* 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.[23] Tujuan lainnya bisa jadi adalah terlepas dari motif utama seperti menurunkan pendapatan moneter atau pengumpulan informasi (baik untuk konvensional atau serangan elektronik).

Keempat, serangan teroris menggunakan media internet dapat dilakukan kapan saja. Waktu serangan juga bisa dilakukan dengan memanfaatkan momentum yang tepat agar ketakukan bisa menyebar luas dikalangan masyarakat. Dengan kata lain, waktu serangan akan berkorelasi dengan tujuan, kemampuan, dan faktor rentannya sistem keamananan dari jaringan yang dijadikan alat atau sasaran serangan. Misalnya, situasi gejolak politik yang tidak menentu, menjadikan gerakan ini mendapat tempat dalam melancarkan aksi

---

[19] Andrew M. Colarik, *Cyber Terrorism: Political and Economic Implications,* USA, Idea Group Publishing, 2006, hlm. 15

[20] Ufran, "Kebijakan Antisipatif Hukum Pidana untuk Penanggulangan *Cyber Terrorism*", *Jurnal Masalah-Masalah Hukum,* Vol. 43, No. 4, 2014, hlm. 531-532

[21] *Ibid*

[22] Phillip W. Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," dalam Marianne Wade dan Almir Maljeviæ (Ed), *A Waron Terror? The European Stanceona New Threat, Changing Laws and Human Rights Implications,* New York, Springer, 2015, hlm. 52-56

[23] *Ibid*

terorisme siber. Situasi gejolak politik yang tidak menentu merupakan momentum yang sering dimanfaatkan oleh kelompok terorisme siber.

Kebijakan Hukum Pidana terhadap Terorisme Siber

Penanggulangan kejahatan di masyarakat, tentunya tidak dapat dipisahkan dari konteks kebijakan penal dan non-penal. Kebijakan penal (*penal policy*) diartikan sebagai usaha yang rasional untuk menanggulangi kejahatan dengan menggunakan sarana hukum pidana. Istilah kebijakan penal mempunyai pengertian yang sama dengan istilah kebijakan hukum pidana (*criminal law policy*) dan politik hukum pidana (*strafrechtspolitiek*).[24]

Kebijakan hukum pidana menurut Sudarto, bagaimana merumuskan hukum pidana yang baik yang akan diberlakukan dalam suatu waktu tertentu.[25] Lebih lanjut Sudarto menegaskan bahwa inti dari kebijakan hukum pidana ialah perbuatan apa yang seharusnya dijadikan tindak pidana, sanksi apa yang sebaiknya dikenakan kepada si pelanggar, dan bagaimana prosedur hukum yang akan ditempuh jika terdapat pelanggaran terhadap ketentuan pidana, sehingga pelaku dapat dikenai sanksi pidana.[26] Sementara menurut Marc Ancel, dimaknai sebagai suatu ilmu sekaligus seni yang mempunyai tujuan praktis untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik agar dijadikan pedoman, baik oleh pembuat undang-undang, pengadilan, serta para penyelenggara atau pelaksana putusan pengadilan.[27]

Kebijakan hukum pidana merupakan manifestasi dari segala usaha untuk merasionalkan hukum pidana dalam bentuk perlindungan terhadap masyarakat. Menurut Barda Nawawi Arief, sekiranya kebijakan hukum pemberantasan terorisme siber dilakukan menggunakan sarana hukum pidana, maka kebijakan tersebut harus diarahkan pada tujuan kebijakan sosial *(social policy),* yang terdiri dari kebijakan atau upaya untuk kesejahteraan sosial *(social welfare policy)* dan perlindungan masyarakat *(social defence policy)*.[28]

Penanggulangan kejahatan dengan menggunakan sarana penal dapat di operasionalisasikan melalui beberapa tahapan, yaitu tahap formulasi (kebijakan legislatif), tahap aplikasi (kebijakan yudikatif), tahap eksekusi (kebijakan eksekutif).[29] Tahap kebijakan formulasi adalah tahap dihasilkannya suatu

---

[24] Salman Luthan, *Kebijakan Kriminalisasi di Bidang Keuangan*, Yogyakarta, FH UII Press, 2014, hlm. 14

[25] Sudarto, *Hukum Pidana dan Perkembangan Masyarakat: Kajian Terhadap Pembaharuan Hukum Pidana*, Bandung, Sinar Baru, 1983, hlm. 20

[26] Sudarto, *Hukum dan Hukum Pidana,* Bandung, Alumni, 2007, hlm. 44-48

[27] Barda N. Arief, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara,* Yogyakarta, Genta Publishing, 2010, hlm. 132

[28] Barda N. Arief, *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan*, Bandung, PT. Citra Aditya Bakti, 2001, hlm. 73-74

[29] *Ibid*

peraturan hukum yang akan menjadi pedoman pada tahap berikutnya. Tahap aplikasi yaitu tahap penerapan hukum pidana oleh aparat penegak hukum. Sementara kebijakan eksekusi adalah tahap pelaksanaan hukum pidana secara konkret oleh aparat pelaksana pidana. Sementara kebijakan non penal (sarana diluar hukum pidana), bisa melalui pendidikan, dll.

Melihat penjelasan di atas, dapat ditegaskan bahwa pembaharuan hukum pidana *(penal reform)* merupakan bagian dari kebijakan atau politik hukum pidana *(penal policy)*. Latar belakang diadakannya pembaharuan hukum pidana dapat ditinjau dari aspek sosio-politik, sosio-filosofis, sosio-kultural, atau dari berbagai aspek kebijakan (khususnya kebijakan sosial, kebijakan kriminal, dan kebijakan penegakan hukum). Pembaharuan hukum pidana pada hakikatnya harus diarahkan pada perwujudan perubahan dan pembaruan terhadap berbagai aspek dan kebijakan yang melatarbelakangi pembaharuan tersebut. Pembaharuan hukum pidana secara umum mempunyai makna sebagai suatu upaya untuk melakukan reorientasi dan reformasi hukum pidana yang sesuai dengan nilai-nilai sentral sosiopolitik, sosiofilosofis, dan sosiokultural masyarakat Indonesia.

Pertama, upaya penal melalui kebijakan formulasi. Pemerintah dan DPR harus segera membuat aturan khusus mengenai terorisme siber atau setidaknya sinkronisasi aturan sektoral yang mengatur terkait hal tersebut. Pengaturan terorisme siber dalam UU ITE atau UU Telekomunikasi belum sepenuhnya memberi gambaran tentang pengertian, ruang lingkup, dan sanksinya. UU ITE dan UU Telekomunikasi hanya mengatur perbuatan setiap orang yang ada kaitannya dengan kejahatan teknologi informasi dan telekomunikasi, sementara dalam konteks terorisme siber, pelakunya ialah teroris. Sehingga hal tersebut harus mendapat pengaturan khusus, utamanya mengenai berat sanksi yang harus dikenakan terhadap pelaku teroris.

Meskipun kejahatan teknologi, informasi, dan komunikasi bisa dilakukan oleh setiap orang termasuk teroris, namun setidaknya perbuatan yang dilakukan oleh teroris yang menggunakan sarana internet, secara politik hukum pidana harusnya diberikan sanksi yang lebih berat, mengingat bahayanya perbuatan dan cepatnya tindakan. Hal tersebut harus diatur dalam KUHP sebagai induk aturan hukum pidana atau lebih dipertegas dalam UU Terorisme, sebagai peraturan yang mengatur terorisme.

Oleh karenanya, KUHP maupun UU Terorisme harus segera di revisi, mengingat aturan tersebut sangat konvensional sehingga belum menyentuh yurisdiksi tindak pidana yang umumnya lintas negara yang merupakan akar dari tindakan terorisme siber. Harmonisasi UU Sektoral tersebut dirasa penting, mengingat negara lain sudah lebih tegas dalam mengatur hal tersebut. Misalnya

Amerika dan Australia, yang dapat menjerat setiap orang dan setiap warga negara, yang menyerang negaranya tanpa melihat dimana yurisdiksi orang itu berada.[30]

Masalah yurisdiksi ini penting ditegaskan dalam pengaturan terorisme siber, khususnya di Indonesia. Dalam konteks itu, RUU KUHP telah mengadopsi hal tersebut dalam Asas Wilayah atau Teritorial sebagaimana diatur dalam Pasal 4. Meskipun demikian, berlakunya asas tersebut dalam RUU KUHP tidak serta membuat penegakan hukum terorisme siber menjadi mudah. Barbara Etter, dalam tulisannya berjudul *Critical Issues in High Tech Crime,* mengingatkan hal penting terkait masalah yurisdiksi, yakni pentingnya konsensus global mengenai jenis-jenis CRC *(Computer Related Crime)* dan harmonisasi hukum acara/prosedural di berbagai negara, mengingat sifat transnasional dari *computer crime.*[31]

Kedua, upaya penal melalui kebijakan aplikasi. Dalam konteks ini, pentingnya keahlian aparat penegak hukum untuk melakukan investigasi menggunakan sistem komputer. Karena pada dasarnya, mereka yang diselidiki (penyelidikan dan penyidikan) merupakan seseorang yang mempunyai keahlian dalam bidang komputer, termasuk juga pintar mengelabui aparat penegak hukum dalam penggunaan komputer. Selain itu, pentingnya sinkronisasi mekanisme penegakan hukum, bantuan hukum, ektradisi, dan kerja sama internasional dalam melakukan investigasi *cyber crime.*

Dalam penanganan terorisme siber ini harus dipertegas mengenai kebijakan penegakan hukumnya, apakah ditangani secara khusus oleh Kepolisian Republik Indonesia, Badan Siber dan Sandi Negara (BSSN), atau Badan Nasional Penanggulangan Terorisme (BNPT). Dalam konteks ini, karena ada banyaknya lembaga yang terlibat, maka alangkah lebih baik jika dibentuk tim atau satuan tugas terpadu untuk mensikronisasi kewenangan diantara para penegak hukum. Harmonisasi kewenangan dari berbagai penegak hukum terhadap penanganan terorisme siber tersebut diharapkan dapat meminimalisir timbulnya konflik kewenangan antar lembaga.

Ketiga, upaya penal melalui kebijakan eksekusi. Narapidana teroris dikategorikan sebagai narapidana *high risk* yang membutuhkan perlakuan dan pembinaan khusus, oleh sebab itu proses penempatan narapidana teroris di lembaga pemasyarakatan harus dilakukan hati-hati karena hal tersebut akan berpengaruh pada keberhasilan pembinaan dan program deradikalisasi. Oleh sebab itu, jangan sampai ada toleransi atau *abuse of power* dari aparat untuk

---

30 Barda N. Arief, *Op. Cit.*, hlm. 108

31 *Ibid*

mengistimewakan atau memberi fasilitas khusus bagi mereka, khususnya fasilitas komputer.

Keempat, upaya non-penal melalui pendekatan teknologi *(techno prevention). Cyber terrorism* adalah jenis kejahatan yang terkait erat dengan teroris yang menggunakan teknologi maju sebagai sarana atau sasaran serangan. Maka upaya yang paling rasional dalam menghadapi model baru dari kejahatan tersebut adalah mengutamakan pendekatan teknologi. Hal tersebut dapat dilakukan dengan cara membatasi akses *(password),* memasang proteksi, sistem pemantau serangan, *back up* data secara rutin, serta penggunaan *enkripsi* untuk meningkatkan keamanan terhadap sistem komputer.[32]

Kelima, upaya non-penal melalui peningkatan kerjasama antar negara *(memory of understanding).* Mengingat karakteristik *cyber crime* tidak mengenal batas-batas negara maka dalam upaya penanggulangannya memerlukan suatu koordinasi dan kerjasama antar negara. *Cyber crime* memperlihatkan salah satu kondisi yang kompleks dan penting untuk diadakannya suatu kerjasama internasional. Meski demikian efektivitas dan efisiensi pelaksanaannya masih perlu dicari format yang tepat, karena seperti kasus-kasus sebelumnya banyak konvensi internasional yang terbentur dalam pelaksanaannya. Salah satu unsur yang menjadi tantangan penerapan suatu konvensi adalah perbedaan persepsi terhadap masalah yang bermuara dari perbedaan kepentingan setiap negara.

Keenam, upaya non-penal melalui program deradikalisasi dunia maya. Pemerintah harus tegas dalam mengatasi tindak pidana terorisme siber, jika memang terdapat program penyebaran paham teroris, maka pemerintah harus segera memblokir situs tersebut. Selain itu, pemerintah juga harus punya tindakan preventif guna meminimalisir gerakan terorisme siber semakin menjamur. Hal tersebut dapat diupayakan pengenalan komputer kepada masyarakat terkait fungsi dan penggunaaannya agar tidak disalahgunakan serta pengenalan penggunaan teknologi yang baik melalui kurikulum dunia pendidikan, khususnya kepada generasi muda agar internet tidak dijadikan bahan coba-coba *(iseng)* untuk kegiatan yang tidak baik.

Penutup

Berdasarkan uraian di atas, maka dapat disimpulkan bahwa terorisme siber merupakan aktivitas teroris dalam dunia maya yang sengaja membuat gangguan terhadap sistem komputer *(cyberspace).* Istilah ini masih kontroversial, sebab belum ada istilah baku untuk mendefinisikannya. Sebagian kalangan menilai

[32] Barda N. Arief, *Sari Kuliah Perbandingan Hukum Pidana*, PT. Raja Grafindo Persada, Jakarta, 2002, hlm. 254-255

bahwa tindakan terorisme siber tidak hanya dilakukan oleh teroris, tetapi juga oleh setiap orang sehingga lebih ke arah kejahatan siber. Ketidakpastian definisi tersebut salah satunya karena tidak ada harmonisasi aturan Internasional maupun nasional dalam pengaturannya yang sektoral (KUHP, UU Telekomunikasi, UU Terorisme, dan UU ITE).

Oleh karena itu, mengingat teknologi selalu berkembang setiap saat, sebaiknya perlu perbaikan aturan (kebijakan formulasi) serta pelatihan mengenai penggunaan teknologi dan informasi terhadap aparat penegak hukum (kebijakan aplikasi) sebagai bagian kebijakan penal. Karena untuk mengungkap tindak pidana terorisme siber tidak hanya dibutuhkan keahlian dalam bidang hukum saja, tetapi juga kemampuan untuk menggunakan teknologi. Sementara dalam upaya non-penal, penanganan terorisme siber dapat melalui program deradikalisasi dunia maya, meningkatkan kerjasama Internasional, serta pentingnya melakukan pendekatan dalam bidang teknologi.

Daftar Pustaka

Buku

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

M. Ramli, Ahmad, *Cyber Law dan HAKI dalam Sistem Hukum di Indonesia*, Bandung, Refika Aditama, 2004.

N. Arief, Barda, *Kebijakan Legislatif dalam Penanggulangan Kejahatan dengan Pidana Penjara,* Yogyakarta, Genta Publishing, 2010.

_____, *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan*, Bandung, PT. Citra Aditya Bakti, 2001.

_____, *Sari Kuliah Perbandingan Hukum Pidana*, Jakarta, PT. Raja Grafindo Persada, 2002.

_____, *Tindak Pidana Mayantara*: *Perkembangan Kajian Cyber Crime di Indonesia*, Jakarta, PT. Raja grafindo Persada, 2006.

N. Samad, Alfira, *Analisis Instrumen Cyber Terrorism dalam Kerangka Sistem Hukum Internasional*, Makassar, Universitas Hasanuddin, 2014.

Luthan, Salman, *Kebijakan Kriminalisasi di Bidang Keuangan*, Yogyakarta, FH UII Press, 2014.

Raharjo, Agus, *Cybercrime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi,* Bandung, Citra Aditya Bahkti, 2002.

S. Adji, Indriyanto, *Terorisme dan HAM dalam Terorisme: Tragedi Umat Manusia,* Jakarta, O.C. Kaligis & Associates, 2001.

Sudarto, *Hukum Pidana dan Perkembangan Masyarakat: Kajian Terhadap Pembaharuan Hukum Pidana*, Bandung, Sinar Baru, 1983.

_____, *Hukum dan Hukum Pidana,* Bandung, Alumni, 2007.

W. Brunst, Phillip, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," dalam Marianne Wade dan Almir Maljeviæ (Ed), *A Waron Terror? The European Stanceona New Threat, Changing Laws and Human Rights Implications,* New York, Springer, 2015.

Wisnubroto, Aloysius, *Kebijakan Hukum Pidana Dalam Penanggulangan Penyalahgunaan Komputer,* Yogyakarta, Penerbit Universitas Atma Jaya Yogyakarta, 1999.

Jurnal

Ari Mahartha dan Made Mahartayasa, "Pengaturan Tindak Pidana Terorisme dalam Dunia Maya *(Cyber Terrorism)* Berdasarkan Hukum Internasional, *Jurnal Kertha Negara,* Vol. 4, No. 6, 2016.

Bayu Widianto, "Dampak Serangan Virtual ISIS *Cyber-Caliphate* Terhadap Amerika Serikat", *International and Diplomacy,* Vol. 2, No. 2, 2017.

Eka L. Marpaung, Mila Astuti, dan Ali Ibrahim, "Analisis *Cyber Law* dalam Pemberantasan *Cyber Terrorism* di Indonesia", *Prosiding Annual Research Seminar Computer Science and ICT,* Vol. 3, No. 1, 2017.

Eska N. Sarinastiti dan Nabila K. Vardhani, "Internet dan Terorisme: Menguatnya Aksi Global *Cyber Terrorism* Melalui New Media", *Jurnal Gama Societa,* Vol. 1, No. 1, 2018.

Mohammad Ngafifi, "Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya", *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, Vol. 2, No. 1, 2014.

Ufran, "Kebijakan Antisipatif Hukum Pidana untuk Penanggulangan *Cyber Terrorism*", *Jurnal Masalah-Masalah Hukum,* Vol. 43, No. 4, 2014.

Internet

James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", dalam *https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf*

Marquerite A. Sapiie, "Indonesia Joins World to Fight Cyber Terrorism" dalam *https://www.thejakartapost.com/news/2015/12/10/indonesia-joins-world-fight-cyber -terrorism.html*

Oik Yusuf, "Rumah Sakit Indonesia jadi Korban Terorisme *Cyber*" dalam *https://tekno.kompas.com/read/2017/05/13/17180077/rumah.sakit.indonesia.jadi.korban.terorisme.cyber.?page=all*

Zahri bin Yunos, "Addresing Cyber Terrorism Threats" dalam *https://observatoire-fic.com/en/addressing-cyber-terrorism-threats-by-zahri-bin-yunos-cybe rsecurity-malaisia/*

Makalah, Pidato

Burhan Bungin , "Cybercommunity, Konstruksi Sosial Teknologi Telematika Atas Realitas Masyarakat Maya", *Pidato Pengukuhan Jabatan Guru Besar dalam Ilmu Sosiologi Komunikasi Pada Universitas 17 Agustus 1945 Surabaya*, 2002.

Peraturan Perundang-undangan

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 15 Tahun 2003 tentang Perppu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang sebagaimana telah diubah dengan Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Perppu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang