Vol. 10, No. 2, 2024, pp. 308-316
DOI: https://doi.org/10.29210/020243153

Contents lists available at Journal IICET

JPPI (Jurnal Penelitian Pendidikan Indonesia)
ISSN: 2502-8103 (Print) ISSN: 2477-8524 (Electronic)

Journal homepage: https://jurnal.iicet.org/index.php/jppi

Pengaturan *cyber terrorism* ditinjau dari perspektif *organizational transnational crime*

Putu Sekarwangi Saraswati*), I Nengah Susrama
Fakultas Hukum Universitas Mahasaraswati Denpasar, Indonesia

Article Info

Article history:

Received Aug 09th, 2023
Revised Nov 27th, 2023
Accepted May 03rd, 2024

Keyword:

Transnastinal crime,
Cyber terrorism,
Cyber crime,
Informasi teknologi

ABSTRACT

Perkembangan teknologi dan informasi yang kian pesat tidak hanya memberi akses kemudahan bagi masyarakat, namun juga diikuti oleh munculnya kejahatan baru yang salah satunya adalah cyber terrorism. Tujuan penelitian ini untuk menganalisis pengaturan cyber terrorism ditinjau dari perspektif organizational transnational crime; dan aksi global cyber terrorism. Metode penelitian yang digunakan adalah jenis penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi kepustakaan. Analisis data dalam penelitian ini yaitu Keseluruhan data yang terdiri dari data primer dan data sekunder akan diolah dan dianalisis secara kualitatif. Hasil penelitian menunjukkan Pengaturan cyber terrorism ditinjau dari perspektif organizational transnational crime menunjukkan bahwa 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; Aksi global cyber terrorism seiring dengan kecanggihan teknologi era digital semakin menguat dan semakin beragam aksi yang bisa dilakukannya. Sejauh ini, aksi cyber-terrorism dilakukan mulai dengan mengintimidasi pemerintah dan masyarakat sipil dengan menganggu sistem jaringan infrastruktur; melakukan serangan, pembunuhan, dan propaganda dengan akurasi yang tinggi tanpa terdeteksi tempat dan media yang digunakan.

Corresponding Author:

Putu Sekarwangi Saraswati,
Universitas Mahasaraswati Denpasar
Email: sekarwangisaraswati@gmail.com

Pendahuluan

Terorisme bukan lagi permasalahan lokal dari negara-negara tertentu tapi isu yang mencakup sejumlah aspek internasional. Terorisme merupakan fenomena internasional, maka tanggapan-tanggapannya juga harus internasional(Ganor, 2002). Para teroris tersebar dimana-mana dengan menggunakan media sebagai alat komunikasi mereka maupun sebagai media komunikasi mereka dalam mengkomunikasikan keberadaan mereka pada seluruh dunia. Media komunikasi mereka mulai dari menggunakan buku, majalah, surat kabar, musik, film, software, games mulai dari bentuk fisik (hardcopy) sampai dalam bentuk softfile yang disebarkan ke seluruh dunia(Brenner, 2002).Perkembangan era globalisasi yang memunculkan media Internet menjadikan

media komunikasi yang digunakan teroris semakin berkembang. Dengan kecanggihan teknologi yang semakin berkembang seiring perkembangan globalisasi, sifat lintas batas negara dari tindak pidana terorisme semakin nyata adanya. Bentuk terorisme yang memiliki karakteristik lintas batas negara yang demikian lazim disebut dengan istilah cyber terrorism. Sifat virtual dari cyber space sangat memungkinkan aksi terorisme dilakukan dengan melintasi batas-batas negara (borderless)(Dikdik M. Elisatris Gultom, 2005).Mereka berusaha menyesuaikan kemampuan mereka dengan perkembangan teknologi komunikasi dan informasi yang ada. Kemudian, terjadilah tranformasi dari penggunaan media konvensional ke media baru, yakni Internet yang memunculkan fenomena cyber terrorism. Cyber terrorism ini menjadi isu dunia yang menuntut seluruh Negara untuk mampu menguasai dunia Internet guna mengetahui tindakan teroris. Semakin pesat perkembangan teknologi media baru, semakin canggih juga media yang digunakan oleh teroris dan semakin besar pula tindakan terorisme yang bisa terjadi.

Selain itu kejahatan yang ditimbulkan oleh internet juga dapat berdimensitransnasional yang biasa disebut dengan transnational crime (kejahatan transnasional). Kejahatankejahatanadalah kejahatan yang pada hakikatnya berdimensi nasional namunmemiliki karakteristik transnasional atau lintas negara(Rani, 2012). Locus delicti terjadinyakejahatan transnasional pada kenyataannya masih berada di dalam batas-bataswilayah sebuah negara, namun dalam pelaksanaannya kejahatan transnasionalmelibatkan urusan- urasan milik negara-negara lain, sehingga seolah-olah terdapatdua atau lebih negara yang memiliki kepentingan terhadap kejahatan tersebut. Jadiinti sebenarnya dari kejahatan transnasional adalah kejahatan tersebut berdimensi nasional, namun dikarenakan adanya keterkaitan dengan kepentingan negara lain maka tampaklah sifatnya yang transnasional(Parthiana, 2006).

Salah satu kejahatan yang berhubungan dengan internet serta memiliki dimensi transnasional adalah kejahatan yang bisa kita sebut dengan istilah cybercrime atau kejahatan melalui jaringan internet. Menurut Kementrian Luar Negeri Republik Indonesia kejahatan cybercrime termasuk dalam kategori kejahatan transnasional, mengingat salah satu ciri khusus kejahatan cybercrime adalah kejahatan ini dilakukan secara online dan seringkali tidak dengan jelas dikaitkan ke lokasi geografis manapun, sehingga seringkali melampaui batas-batas negara lain. Dan salah satu ciri kejahatan transnasional adalah dilakukan melampaui batas negara, jadi cybercrime ini sudah memenuhi salah satu syarat untuk disebut sebagai salah satu bagian dari kejahatan transnasional.

Selain alasan tersebut, pada tahun 2010 Conference of States Parties (CoSP)United Nation Convention Against Transnational Organized Crime (UNTOC) menyebutkan bahwa terdapat beberapa kejahatan baru yang teridentifikasi sebagai Kejahatan Lintas Negara Baru dan Berkembang (New and Emerging Crimes), kejahatan tersebut antara lain kejahatan dunia maya, kejahatan terkait identitas, penjualan cagar budaya secara gelap, kejahatan lingkungan, perompakan di atas laut, dan perdagangan gelap organ tubuh. Kejahatan Lintas Negara Baru saat ini diberi perhatian khusus oleh dunia internasional dikarenakan angka terjadinya kejahatan tersebut cukup tinggi, kerugian yang ditimbulkan besar serta modus operandi yang digunakan juga sangat beragam. Cybercrime adalah serangan kriminal yang melibatkan atau terjadi pada cyberspace, wilayah yang sangat halus yang tercipta ketika komputer dan orang terhubung melalui jaringan elektronik yang membentang di seluruh dunia. Cybercrime yang muncul sebagai persoalan kejahatan dan pengadilan internasional merupakan sisi buruk dari masuknya teknologi komunikasi digital, terutama internet, ke dalam kehidupan sehari-hari dan perdagangan global(Natarajan, 2015).Pengertian cybercrime berkembang terus-menerus secara linear dengan perkembangan kejahatan di internet. Pada mulanya cybercrime hanya mencakup kejahatan computer crime, yaitu kejahatan yang ditargetkan pada komputer atau komputer dimanfaatkan sebagai alat guna melakukan kejahatan. Namun saat ini ruang lingkup cybercrime mencakup berbagai kejahatan yang lebih bervariasi dan luas, tidak hanya bentuk computer crime saja tetapi juga juga bentuk-bentuk kejahatan lain yang termasuk computer related crime.

Cyber terrorism adalah kejahatan yang dilakukan oleh oknum yang bermaksud mengedepankan tujuan sosial, agama atau politik namun dengan cara menyebabkan rasa takut yang meluas atau dengan merusak atau menggangu informasi infrastruktur yang penting. Berdasarkan penjelasan jenis-jenis cybercrime, cyber terrorism merupakan kejahatan yang baru muncul (Samuel, 2009). Kejahatan ini menggunakan media komputer dalam menyebarkan ideologi yang bersifat terror guna menjalankan aksi kejahatan teroris di internet (Sri Ayu, 2015). Internet menyebutkan istilah cyber terrorism sebagai kegiatan dimana sekelompok teroris menggunakan media cyberspace guna melaksanakan aksi terorisme. Jadi cyber terrorism sendiri terdiri dari unsur cyberspace dan terorisme (Richard and Sarah, 2006). Pengertian cyberspace tidak terbatas kepada dunia yang tercipta akibat dari terjadinya hubungan melalui internet. Internet dapat menyebarkan informasi yang cepat dengan sedikit resiko, serta tidak membutuhkan biaya yang mahal guna melakukan perekrutan yang potensial, sehingga potensi memperoleh partner yang prospektif dalam organisasi teroris menjadi mudah(Conway, 2014).

Sedangkan terorrisme dalam penjelasan Convention of The Organization of theIslamic Confrnece on Combating Internasioanl Terrorism 1999, merupakan tindakan yang berbentuk kekerasan atau ancaman, yang dilakukan guna menteror orang lain atau memberikan ancaman yang mencelakakan hidup banyak orang, harga diri, kebebasan, keamanan dan hak yang mereka miliki, atau mengeksploitasi harta, sumber daya alam, fasilitas milik pribadi atau publik, atau menguasai, merampas, membahayakan sumber nasional atau fasilitas internasional, atau mengancam stabilitas, integritas territorial, kesatuan politis serta kedaulatan sebuah negara(Dayan, 2015).Denning berpendapat bahwa cyberterrorism adalah: "Serangan yang melanggar hukum dan ancaman serangan terhadap komputer, jaringan, dan informasi yang tersimpan di dalamnya ketika dilakukan untuk mengintimidasi atau memaksa pemrintah atau orang- orangnya untuk melanjutkan politik atau kepentingan sosial(Murat et. all., 2011)."

Cyber terrorism melakukan serangan terhadap apa saja yang terhubung dengan internet terutama objek vital milik pemerintah yang dapat menggangu fungsinya bahkan dapat membuat jatuh korban yang lebih besar daripada terorisme dengan modus opernadi konvensional (Agis J.A, 2014). Negara dituntut untuk mampu menguasai dunia Internet guna mengetahui tindakan teroris dikarenakan cyberterrorism telah menjadi isu dunia. Semakin pesat sebuah teknologi baru berkembang, maka semakin canggih media serta modus opernadi yang digunakan oleh teroris sehingga semakin besar kesempatan tindak pidana terorisme bisa terjadi.

Berbagai bentuk tindak pidana yang digunakan sebagai modus operandi yang digunakan teroris dalam melakukan tindak pidana cyber terrorism juga menjadi salah satu alasan mengapa perlu adanya regulasi khusus guna penegakan tindak pidana cyber terrorism(Satriana & Pramestiani, 2020). Salah satu cara atau modus operandi yang digunakan oleh teroris dalam melakukan tindak pidana cyber terrorism adalah penyebaran propaganda, hukum nasional maupun hukum internasional belum mengatur mengenai kejahatan penyebaran propaganda tersebut, padahal efek dari kejahatan propaganda tersebut cukup besar dan berpengaruh bagi kehidupan sebuah negara. Apabila regulasi mengenai salah satu bentuk cyber terrorism tersebut belum tersedia, maka akan menyulitkan sebuah negara dalam hal penegakan kejahatannya.

Pentingnya regulasi mengenai cyber terrorism juga tidak hanya disebabkan karena belum adanya regulasi khusus yang mengatur tindak pidana tersebut, namun juga dikarenakan posisi tindak pidana cyber terrorism yang merupakan salah satu bentuk dari kejahatan transnasional terorganisir. Menurut Rahmani Dayan dalam bukunya, terdapat karakteristik khusus yang dimiliki oleh terorisme namun tidak dimiliki oleh kejahatan-kejahatan konvensional lain, tindak pidana tersebut dilakukan secara terstuktur dan melebar serta terorganisasi sehingga menjadi sebuah ancaman yang sangat serius bagi masyarakat, bangsa dan negara. Oleh karena itu Cyber terrorism termasuk dalam kategori "Transnational OrganizedCrime". Luasnya cakupan dari kasus cyber terrorism ini membuat hukum nasional negara-negara yang bersangkutan tidak akan cukup untuk menyelesaikan kasus cyber terrorism. Selain itu masuknya tindak pidana cyber terrorism kedalam kategori kejahatan transnasional terorganisir ini membuat pengaturan yang mengatur tindak pidana ini harus lebih banyak.

Penelitian terkait dengan cyber terrorism pernah diteliti oleh Juli Sapta Eka Putri dengan judul "Kejahatan Cyber Terrorism dalam Hukum Pidana di Indonesia"(Putri, 2019). Penelitian Juli Sapta Eka Putri dengan penelitian yang akan dilakukan memiliki persamaan dan perbedaan. Persamaannya kedua penelitian ini sama-sama meneliti tentang cyber terrorism. Perbedaannya jika pada penelitian Juli Sapta Eka Putrimeneliti mengenai kejahatan cyber terrorism dalam hukum pidana di Indonesia, sedangkan pada penelitian yang akan dilakukan meneliti tentang pengaturan cyber terrorism ditinjau dari perspektif organizational transnational crime.Selain itu, penelitian lainnya dilakukan oleh (Sarinastiti & Vardhani, 2017)dengan judul "Internet Dan Terorisme: Menguatnya Aksi Global Cyber Terrorism Melalui New Media. Penelitian Eska Nia Sarinastiti dan Nabilla Kusuma Vardhani dengan penelitian yang akan dilakukan memiliki persamaan dan perbedaan. Persamaannya kedua penelitian ini sama-sama meneliti tentang cyber terrorism. Perbedaannya jika pada penelitian Eska Nia Sarinastiti dan Nabilla Kusuma Vardhanimeneliti mengenai internet dan terorisme: menguatnya aksi global cyber terrorism melalui new media, sedangkan pada penelitian yang akan dilakukan meneliti tentang pengaturan cyber terrorism ditinjau dari perspektif organizational transnational crime.

Selanjutnya penelitian Ari Mahartha dan Made Mahartayasa dengan judul "Pengaturan Tindak Pidana Terorisme Dalam Dunia Maya (Cyber-Terrorism) Berdasarkan Hukum Internasional"(Ari Mahartha, 2016). Dalam penelitian Ari Mahartha dan Made Mahartayasa dengan penelitian yang akan dilakukan memiliki persamaan dan perbedaan. Persamaannya kedua penelitian ini sama-sama meneliti tentang cyber terrorism. Perbedaannya jika pada penelitian Ari Mahartha dan Made Mahartayasa meneliti mengenai pengaturan tindak pidana terorisme dalam dunia maya (cyber-terrorism) berdasarkan hukum internasional, sedangkan pada penelitian ini adanya pembaharuan untuk dilakukannyapenelitian yaitu tentang pengaturan cyber terrorism ditinjau dari perspektif organizational transnational crime.Berdasarkan persamaan dan perbedaan penelitian-penelitian sebelumnya dengan penelitian ini seperti diuraikan di atas, maka dapat dinyatakan

bahwa penelitian ini berbeda baik substansi maupun metodologinya dengan penelitian-penelitian sebelumnya. Oleh karena itu, maka peneliti ingin melakukan penelitiandengan tujuan untuk menganalisispengaturan cyber terrorism ditinjau dari perspektif organizational transnational crime, serta menganalisis aksi global cyber terrorism.

Metode

Metode penelitian yang digunakan dalam penelitian ini adalah jenis penelitian hukum normatif. Penelitian hukum normatif (normative legal research) merupakan penelitian yang dilakukan dengan cara mengkaji peraturan perundang-undangan yang berlaku atau diterapkan terhadap suatu permasalahan hukum tertentu. Penelitian hukum normatif meneliti hukum dari perspektif internal dengan objek penelitiannya adalah norma hukum(Diantha, 2017). Penelitian normatif seringkali disebut dengan penelitian doktrinal, yaitu penelitian yang objek kajiannya adalah dokumen peraturan perundang-undangan dan bahan pustaka(Marzuki, 2013). Penelitian hukum normatif juga disebut penelitian yang difokuskan untuk mengkaji penerapan kaidah-kaidah atau norma dalam hukum positif(Ibrahim, 2012). Menurut I Made Pasek Diantha penelitian hukum normatif berfungsi untuk memberi argumentasi yuridis ketika terjadi kekosongan, kekaburan dan konflik norma. Lebih jauh ini berarti penelitian hukum normatif berperan untuk mempertahankan aspek kritis dari keilmuan hukumnya sebagai ilmu normatif. Pendekatan yang digunakan adalah pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi kepustakaan. Analisi data dalam penelitian ini yaitu Keseluruhan data yang terdiri dari data primer dan data sekunder (bahanhukum primer, sekunder dan tersier) akan diolah dan dianalisis secara kualitatif.

Hasil dan Pembahasan

Pengaturan *Cyber Terrorism* Ditinjau dari Perspektif *Organizational Transnational Crime*

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(Samad, 2014).

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.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:

"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 terrorismand 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. 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.Harmonisasi pengaturan hukum mengenai cyber terrorism amat penting untuk dilakukan karena

peraturan perundang-undangan nasional tidak boleh bertentangan dengan hukum internasional(Wijaya, 2018). 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.

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 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(Golose, 2015).

Di Indonesia, tindak pidana cyber terrorism tidak diatur di dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun peraturan perundang-undangan yang mengatur di bidang terorisme, terutama dalam Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme. 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. Karakteristik pertama cyber terrorism adalah tindakan teror terhadap sistem komputer, jaringan, dan/atau basis dan informasi yang tersimpan dalam komputer. Adapun bentuk-bentuk perbuatan yang termasuk kategori ini antara lain: 1) *Unauthorized access to computer system and service*, yaitu kejahatan menggunakan system komputer melalui jaringan secara tidak benar dan tanpa ijin dari pemilik; 2) *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; 3) *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; 4) *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 computer; 5) *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 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (selanjutnya disebut UU ITE Perubahan), seperti yang diuraikan di bawah ini: 1) Pasal 30 UU ITE Perubahan mengatur tentang tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun. Konstruksi perbuatan dalam rumusan pasal ini menjelaskan bahwa tindakan tidak sah/illegal yang dilakukan oleh seseorang terhadap sistem elektronik milik orang lain dengan tujuan untuk memproleh informasi/dokumen elektronik dan/atau upaya pembobolan, penerobosan, dan penjebolan yang melanggar dan melampaui sistem pengamanan; 2) Pasal 32 dan Pasal 33 UU ITE Perubahan yang mengatur tentang perlindungan terhadap suatu informasi dan/atau dokumen elektronik baik milik orang lain atau milik publik yang bersifat rahasia.

Sifat melawan hukum dalam Pasal 30 UU ITE Perubahan tersebut memiliki dua corak, yakni melawan hukum objektif dan melawan hukum subjektif. Melawan hukum objektif berarti komputer dan/ atau sistem komputer tersebut bukan milik pelaku dan perbuatan mengakses komputer dan/atau sistem elektronik tersebut tanpa izin pemilik/tanpa hak. Sama halnya dengan Pasal 30 UU ITE Perubahan, Pasal 32 UU ITE Perubahan juga memiliki dua corak sifat melawan hukum. Sifat melawan hukum yang objektif dalam rumusan pasal ini terdapat pada unsur objeknya, bahwa Informasi Elektronik dan/atau Dokumen Elektronik tersebut milik orang lain. Agar rumusan tersebut memenuhi sifat melawan hukum yang objektif, maka frasa milik orang lain tersebut harus dibuktikan dan dipastikan keberadaannya melalui perbuatan mengubah dan sebagainya tersebut harus tidak ada izin dari pemiliknya.

Sedangkan sifat melawan hukum yang subjektifnya terletak pada keadaan batin si pelaku terhadap sifat melawan hukum objektifnya perbuatan. Pelaku mengetahui bahwa perbuatan Yang hendak diperbuatnya adalah yang mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, serta memindahkan, dan menyembunyikan dengan cara apapun suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik sebagai perbuatan yang tercela(Adami & Ardi, 2011). Sifat melawan hukum dalam Pasal 33 UU ITE Perubahan terletak pada akibat perbuatan tersebut, yakni perbuatan pelaku tersebut akan mengakibatkan terganggunya atau tidak bekerjanya sistem elektronik tersebut sebagaimana mestinya.

Pasal 30, Pasal 32, dan Pasal 33 UU ITE Perubahan 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). Cyber terrorism menurut Dening didalam (Jondong, 2020)adalah perbuatan melawan hukum yang dilakukan dengan menyerang komputer, jaringan, dan informasi yang tersimpan di dalamnya serta bertujuan untuk mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik dan sosial atau jika penulis artikan secara singkat adalah terorisme yang dilakukan melalui dunia maya atau teroris yang menggunakan teknologi siber, sedangkan terorisme siber adalah perbuatan seseorang atau beberapa orang yang bertujuan untuk melakukan serangan siber. Prinsip anonimitas menjadi faktor yang menjadikan perbedaan antara istilah tersebut semakin menghilang(Lubis, 2017).

Terorisme siber cenderung tidak mempunyai anggota kelompok dalam jumlah besar, sedangkan terorisme yang menggunakan dunia maya mempunyai banyak anggota bahkan cabang yang tersebar di seluruh dunia. Serangan yang dilakukan atas dasar terorisme siber tidak diafiliasi dengan kelompok teroris manapun di seluruh dunia, meskipun terdapat motif politik di dalamnya. Sedangkan, terorisme yang menggunakan dunia maya adalah terorisme yang memanfaatkan kemajuan teknologi dan informasi sebagai media untuk melakukan aktivitas 9P mereka, yaitu propaganda, perekrutan, penyediaan logistik, pelatihan, pembentukan para militer melawan hukum, perencanaan, pelaksanaan serangan teroris, persembunyian, dan pendanaan. Relevansi Pasal 30, Pasal 32, dan Pasal 33 UU ITE Perubahan 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 Perubahan 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 Perubahan untuk menanggulangi tindak pidana cyber terrorism. Selanjutnya, karakteristik kedua, yakni cyber terrorism sebagai pemanfaatan internet oleh para teroris untuk keperluan organisasi dan media teror kepada pemerintah dan masyarakat, dapat digali dan dianalisa pengaturannya dalam UU No 15 Tahun 2003, sebagaimana rumusan dalam Pasal 6 UU No 15 Tahun 2003 Tindak Pidana Terorisme. Pertanggungjawaban pidana merupakan suatu terusan celaan bagi pelaku atas tindak pidana yang telah dilakukannya(Permana & Heniarti, 2022). Celaan dalam pertanggungjawaban pidana dibagi atas celaan secara objektif dan celaan secara subjektif. Celaan secara objektif berarti pelaku telah melakukan tindak pidana (perbuatan yang dilarang atau melawan hukum dan dapat diberi pidana berdasarkan hukum yang berlaku atau asas legalitas), sedangkan celaan secara subjektif berarti pelaku patut untuk dicela atau diminta pertanggungjawabannya atas tindak pidana yang telah dilakukannya.

Aksi Global *Cyber Terrorism*

Cyber-terrorism merupakan konvergensi dari terorisme dan cyberspace. Cyber-terrorism merupakan penggunaan peralatan jaringan komputer untuk mengganggu sistem infrastruktur Negara (energi, transportasi, operasional pemerintahan, dan sejenisnya) atau untuk mengintimidasi pemerintahan atau sekelompok masyarakat sipil(Tan, 2003). Cyberspace merupakan metode pengiriman pesan yang menarik untuk teroris. Akses dengan cyberspace lebih mudah diperoleh dibandingkan media konvensional. Hanya satu yang dibutuhkan, yakni komputer yang terhubung dengan Internet. Namun, cyberterrorist juga memerlukan level tinggi untuk menguasai komputer. Kemampuan cyberspace yang dapat ditembus juga memfasilitasi cyber-terrorism.Cyber space dapat digunakan untuk mengalahkan sistem dan menghindari inspeksi(Mohsin, n.d.). Teroris di beberapa Negara dapat bertukar e-mail dengan sedikit ketakutan akan diawasi. Teroris bisa bertemu secara online dan menghindari pengecekan imigrasi dengan menggunakan cyber space. Jadi, cyberspace menawarkan para teroris keamanan yang lebih kuat dan fleksibilitas operasional. Mereka dapat meluncurkan serangan dari hampir semua tempat di dunia tanpa secara langsung mengekspos diri mereka yang membahayakan diri mereka secara fisik. Mereka tidak terhambat oleh regulasi lagi. Bahkan, pada tahun 2002 menurut peneliti Microsoft, mereka memiliki taktik dengan sering kali menghilang begitu saja secara cepat dan mengganti situs mereka dengan alamat yang berbeda lagi dengan tujuan menghindari pengawasan dari pihak pemerintah maupun intelejen tapi konten tetap sama(Sarinastiti & Vardhani, 2017).

Selain itu, cyber space juga menawarkan teroris kemampuan untuk menyerang secara struktur dengan ketepatan yang tinggi. Penggunaan Internet oleh teroris memberikan cara yang murah untuk mereka menyebarkan propaganda mereka tanpa mempermasalahkan faktor geografis yang jauh maupun sulit dijangkau. Adanya Internet, video-video aksi terorisme mereka dapat dilihat jutaan orang, berbagai gambar dan perkataan mampu tersebarkan secara bebas tanpa ada gatekeeper yang harus mereka lalui seperti media massa. Al- Qaeda mengadopsi Internet sebagai medium yang terbaik untuk mengirim dan menerima pesan pada audiens yang tersebar di beragam tempat di dunia.Penggunaan cyberspace juga membiarkan teoris mengirimkan sebuah serangan yang mencakup beberapa serangan yang berurutan hanya dari satu tempat(Efendi, 2022). Teroris bisa melaksanakan aksinya dari jarak yang sangat jauh, bahkan beda benua atau Negara dengan Internet. Bahkan juga jika mereka menggunakan komputer dekat dengan area sasarannya, teroris tidak perlu ada ditempat lokasi sehingga penggunaan cyberspace berarti aksinya tidak perlu mengorbankan anggota mereka. Di Timur Tengah, website dari kelompok militan Islam, Hezbollah, diciptakan oleh para pendukung Hamas untuk mengumumkan pembunuhan mereka terhadap sekelompok Yahudi. Cyber war terjadi antara pihak Arab dengan Yahudi. Selain itu, serangan secara cyber terjadipada komputer militer Amerika Serikat ketika berada di Kosovo dalam rangka melindungi Negara tersebut dari serangan Serbia untuk meninggalkan Negara tersebut(Lewis, 2002). Bahkan, secara lebih detail bukan hanya propaganda saja, Internet digunakan sebagai media publikasi untuk penggalangan dana, membicarakan target, dan koordinasi melakukan serangan(Banez, 2010). Para teroris pun semakin pintar menggunakan fasilitas perpustakaan online dimana banyak informasi didalamnya tentang material maupun cara membuat bom. Bahkan, kemungkinan mereka bisa membuat perpustakaan online sendiri yang terselubung dan menjadi sumber berbagai anggota kelompok teroris untuk melakukan aktivitas terorismenya. Kelompok teroris di seluruh dunia bisa mengaksesnya dengan mudah.

Pada tahun 1996, kelompok Hamas Palestina dilaporkan melakukan "chat room dan e-mail" untuk merencanakan dan berkoordinasi dalam operasinya di Gaza dan Lebanon. Selama periode yang sama, Hezbollah Lebanon membangun sejumlah situs untuk melaporkan keberhasilan serangannya melawan Israel. Internet menguntungkan untuk komunikasi dan operasional mereka. Kelompok Al-Qaeda memiliki situs salah satunya www.alneda.com, akan tetapi setelah terjadi peristiwa 9/11 situs tidak terdeteksi lagi, tidak terdapat gambar Al-Qaeda. Maka, terjadi pergerakan teroris secara online (terrorism movement) dari satu alamat situs ke alamat lain, dari satu sistem online ke sistem lain. Mereka bisa mengganti sistem mereka dengan mudah ketika mereka mulai terdeteksi oleh pihak pemerintah, khususnya pihak pemerintah dan militer Amerika Serikat.

Berdasarkan temuan Seib dan Janbek menyatakan bahwa Al-Qaeda memiliki produksi operasional sendiri untuk konten online yang disebarkannya, yang bernama As Sahab (The Clouds) yang berfungsi dengan dibawah keamanan yang sangat ketat. Video Osama Bin Laden, Zawahiri, atau juru bicara Al-Qaeda lainnya yang tertembak di lokasi yang terisolasi dibawa menuju tempat yang aman untuk di-upload di Internet dan kemudian video dikirimkan ke fasilitas produksi terakhir Al Sahab, dimana video tersebut di-edit secara grafis dan tambahan subtitle-nya. As Sahab menggunakan peralatan seperti Laptop Sony Vaio dan software yang sangat tinggi kualitasnya dalam melindungi data mereka. Produk video tahap akhirnya adalah video dibawa oleh seorang kurir ke warnet dan di-upload pada beragam situs afiliasi Al-Qaeda. Alamat-alamat Internet tersebut di-publish melalui berbagai forum dan ruang chatting. Kemudian pengikut Al-Qaeda meng-copy-nya dan mendistribusikannya. Sistem ini sudah digunakan sejak tahun 2005, yakni sejak Al-Qaeda berhenti mengirimkan videonya pada stasiun televisi Al-Jazeera dan organisasi pemberitaan lainnya, yang suka meng-edit tidak sesuai faktanya, bahkan menghilangkan video yang dikirimkan oleh Al-Qaeda.

Sebenarnya pemanfaatan Internet oleh teroris bukan hanya dari kelompok teroris Al-Qaeda saja, akan tetapi kelompok lain juga menggunakan seperti Taliban dan Hizbut Tahrir. Namun, keberadaan media online mereka tidak semahir, sekuat dan sebanyak Al- Qaeda. Dengan demikian, seperti yang disimpulkan oleh pihak United Nations Office on Drugs and Crime bahwa penggunaan Internet oleh teroris didasari beberapa tujuan yang mereka harus capai, mencakup penyebaran propaganda (termasuk rekruitmen, radikalisasi, penghasutan), mencari dana, pelatihan, perencanaan (melalui komunikasi rahasia dan informasi terbuka), eksekusi, dan cyberattack. Penggunaan media berbasis Internet ini menunjukkan bahwa para teroris memahami media sebagai alat strategi dan taktik dalam aktivitas teroris mereka. Penggunaan Internet oleh teroris dalam berbagai bentuk pesan baik secara audio visual, gambar, maupun kata-kata secara simultan dan kontinu bertujuan agar masyarakat dunia tetap sadar akan eksistensi para teroris.

Berdasarskan hasil pembahasan yang telah diuraikan di atas, diketahui bahwa pengaturan cyber terrorism ditinjau dari perspektif organizational transnational crime menunjukkan bahwabelum 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 UU ITE jo UU ITE Perubahan.Aksi global cyber terrorism seiring dengan kecanggihan teknologi era digital semakin menguat dan semakin beragam aksi yang bisa dilakukannya. Sejauh ini, aksi cyber-terrorism dilakukan mulai dengan mengintimidasi pemerintah dan masyarakat sipil dengan menganggu sistem jaringan infrastruktur; melakukan serangan, pembunuhan, dan propaganda dengan akurasi yang tinggi tanpa terdeteksi tempat dan media yang digunakan; mengumumkan berbagai aksi radikal pembunuhan dan terror melalui video maupun gambar secara online yang disebarkan melalui akun pribadi mereka; pembuatan online library untuk anggota terroris dalam berbagi ilmu pembuatan bom dan berbagai senjata illegal; dan melakukan hack terhadap beberapa jalur pendanaan. Secara teknologi, jaringan terroris Al-Qaeda dalam aksi cyber-terrorism lebih mahir, kuat dan banyak jumlahnya dibandingkan dengan jaringan terroris lainnya. Penelitian ini sejalan dengan penelitian yang dilakukan oleh (Jondong, 2020) yang menyatakan bahwa hasil penelitian ini mengungkap bahwa diIndonesia tindak pidana cyber terrorismtidak diatur di dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun Peraturan Perundang-Undangan yang mengatur dibidang terorisme. Dalam situasi seperti ini, pelaku tindak pidana cyber terrorismdapat 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 harusdirumuskan secara tegas dan jelas. Selain itu, dalam membentuk kebijakan hukum pidana mengenai tindak pidana cyber terrorism, perbuatan cyber terrorism harus diperhatikan dan dipertimbangkan agar dapat dijadikan tindak pidana dan sanksi dapat dijatuhkan kepada pelaku.

Simpulan

Berdasarkan hasil pembahasan yang telah diuraikan di atas, maka dapat disimpulkan bahwa pengaturan cyber terrorism ditinjau dari perspektif organizational transnational crime menunjukkan bahwabelum terdapat pengaturan secara khusus terkait cyber terrorism dalam hukum internasional. Sedangkan aksi global cyber terrorism seiring dengan kecanggihan teknologi era digital semakin menguat dan semakin beragam aksi yang bisa dilakukannya. Sejauh ini, aksi cyber-terrorism dilakukan mulai dengan mengintimidasi pemerintah dan masyarakat sipil dengan menganggu sistem jaringan infrastruktur; melakukan serangan, pembunuhan, dan propaganda dengan akurasi yang tinggi tanpa terdeteksi tempat dan media yang digunakan; mengumumkan berbagai aksi radikal pembunuhan dan terror melalui video maupun gambar secara online yang disebarkan melalui akun pribadi mereka; pembuatan online library untuk anggota terroris dalam berbagi ilmu pembuatan bom dan berbagai senjata illegal; dan melakukan hack terhadap beberapa jalur pendanaan. Secara teknologi, jaringan terroris Al-Qaeda dalam aksi cyber-terrorism lebih mahir, kuat dan banyak jumlahnya dibandingkan dengan jaringan terroris lainnya.Adapun saran-saran yang dapat diuraikan adalahwalaupun indonesia sudah mempunyai UU ITE jo UU ITE Perubahan untuk menanggulangi masalah kejahatan terhadap komputer akan tetapi, terdapat beberapa norma yang tidak diatur dalam UU ITE jo UU ITE Perubahan yang telah di atur Convention onCybercrime untuk memperluas pengaturan terhadap kejahatan cybercrime oleh karena itu pemerintah disarankan mempertimbangkan untuk meratifikasi Convention on Cybercrime mengingat belom adanya organisasi regional seperti ASEAN yang belom memiliki instrumen hukum mengenai cybercrime.Kepada badan legislatif disarankan untuk mengadakan formulasi tindak pidana cyber terrorism dalam RUU KUHP Nasional beserta penjelasanya secara jelas dan terang sebelum disahkan dan diberlakukan, sehingga dapat mengatasi kekosongan hukum atas bentuk-bentuk kejahatan cyber terrorism yang mengancam keamanan setiap orang dan negara serta dapat mewujudkan kodifikasi hukum pidana nasional.

Referensi

Ari Mahartha, M. M. (2016). Pengaturan Tindak Pidana Terorisme Dalam Dunia Maya (Cyber-Terrorism) Berdasarkan Hukum Internasional. *Jurnal Kertha Negara*, *4*(6), 1–6.

Banez, J. D. (2010). *The Internet And The Homegrown Jihadist Terrorism: Assessing U.S. Detection Techniques*. Naval Postgraduate School California.

Brenner, S. W. (2002). Cyber-Terrorism: How Real Is The Threat? *Media Asia*, *29*(3), 149–154.

Conway, M. (2014). *Cyber Terrorism*. Springer Recuperado.

Dayan, R. (2015). *Sistem Pemidanaan Terhadap Pelaku Tindak Pidana Terorisme Sebagai Extra Ordinary Crime Di*

Indonesia. Genta Publishing.
Diantha, I. M. P. (2017). *Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum*. Prenada Media Group.
Efendi, B. (2022). *Rekonstruksi Regulasi Pencegahan Terorisme Di Era Digitalisasi Yang Berorientasi Pada Keadilan Pancasila*. Universitas Islam Sultan Agung (Indonesia).
Elisatris Gultom, D. M. A. M. (2005). *Cyber Law: Aspek Hukum Teknologi Dan Informasi*. Refika Aditama.
Ganor, B. (2002). Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? *Police Practice And Research: An International Journal*, *3*(4), 287–304.
Golose, P. R. (2015). *Invasi Terorisme Ke Cyberspace*. Yayasan Pengembangan Kajian Ilmu Kepolisian.
Ibrahim, J. (2012). *Teori Dan Metodologi Penelitian Hukum Normatif*. Banyumedia.
Jondong, Z. (2020). Kebijakan Hukum Pidana Bagi Tindak Pidana Cyber Terrorism Dalam Rangka Pembentukan Hukum Positif Di Indonesia. *Jurnal Preferensi Hukum*, *1*(2), 21–27.
Lewis, J. A. (2002). Assessing The Risks Of Cyber Terrorism. *Center For Strategic And International Studies*, 1–12.
Lubis, R. R. (2017). Potensi Pengguna Internet Indonesia Dalam Counter-Cyber Radicalization. *Jurnal Pertahanan & Bela Negara*, *7*(2), 19–34.
Marzuki, P. M. (2013). *Penelitian Hukum*.
Mohsin, A. (N.D.). *Strategi Amerika Serikat Dalam Menghadapi Eskalasi Cyber Power Tiongkok Periode 2011-2015*. Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Islam Negeri Syarif ….
Natarajan, M. (2015). *International And Transnational Crime And Justice*. Cambridge University Pers.
Parthiana, I. W. (2006). *Hukum Pidana Internasional*. Yrama Widya.
Permana, D., & Heniarti, D. D. (2022). Penegakan Hukum Terhadap Tindak Pidana Ilegal Fishing. *Bandung Conference Series: Law Studies*, *2*(1), 680–685.
Putri, S. E. (2019). Kejahatan Cyber Terrorism Dalam Hukum Pidana Di Indonesia. *Jurnal Suara Hukum*, *2*(1), 80–107.
Rani, F. (2012). Strategi Pemerintah Indonesia Dalam Meningkatkan Keamanan Wilayah Perbatasan Menurut Perspektif Sosial Pembangunan. *Transnasional*, *4*(01).
Samad, A. N. (2014). *Analisis Instrumen Cyber Terrorism Dalam Kerangka Sistem Hukum Internasional*. Universitas Hasanuddin Makassar.
Sarinastiti, E. N., & Vardhani, N. K. (2017). Internet Dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism New Media. *Jurnal Gama Societa*, *1*(1), 40–52.
Satriana, I. M. W. C., & Pramestiani, L. P. E. (2020). Kebijakan Formulasi Pencegahan Tindak Pidana Terorisme Di Era Teknologi 4.0. *Kerta Dyatmika*, *17*(2), 12–22.
Tan, K. L. G. (2003). *Confronting Cyber-Terrorism With Cyber Deception*. Naval Postgraduate School California.
Wijaya, R. A. (2018). Kejahatan Transnasional Dalam Cyber Terrorism Menurut Undangâ€"Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Lex Crimen*, *7*(3).