UNJA Journal of LegalStudies
Volume 01 Nomor 02, 2023 (82-99)

Analisis Yuridis Cyber Terrorism Dalam Perspektif UU No. 19 Tahun 2016 Tentang Informasi & Transaksi Elektronik

Submission : 17 April 2023
Revision : 27 Juni 2023
Publication : 30 Juni 2023

Dedy Leonardo Hutagaol
Fakultas Hukum Universitas Jambi. E-mail: dedypol22@gmail.com

Abstract: *Until now, acts of terrorism have involved the use of information technology. With the change in paradigm, acts of terrorism are generally carried out using conventional methods, but currently only by using a laptop or computer with the help of the internet, they carry out a series of acts of terrorism, but there are no regulations that clearly explain the crime of cyber terrorism. ITE law. Apart from that, the regulation of cyber terrorism in Indonesia is currently sectoral as in the Criminal Code (KUHP). The author took this research: 1) To find out the criminal law regulations for eradicating cyber terrorism from the perspective of law number 19 of 2016 concerning information and electronic transactions. 2) To find out and analyze criminal law policies that can be built into preventive cyber terrorism measures. The Normative Juridical Approach is carried out to explain laws that are not needed with data and/or social facts in the perspective of Law Number 19 of 2016 concerning Information and Electronic Transactions relating to this research problem. The results and discussion show that the term cyber terrorism is still controversial, because there is no standard term to define it. One of the reasons for the uncertainty in this definition is because there is no harmonization of international or national rules in sectoral regulations (UU ITE).*

Keywords: *Cyber terrorism; ITE Law; Terrorism; Criminal Law*

Abstrak: Tindakan terorisme tersebut hingga saat ini telah masuk pada penggunaan teknologi informasi. Dengan adanya perubahan paradigma aksi terorisme yang umumya dilakukan dengan menggunakan cara-cara yang konvensional namun saat ini hanya dengan menggunakan sebuah laptop atau komputer dengan bantuan internet mereka melakukan rangkaian aksi terorisme, namun peraturan yang menjelaskan secara jelas terkait dengan kejahatan *cyber terrorism* tidak ada di dalam undang-undang ITE. Selain itu, Pengaturan terorisme siber di Indonesia saat ini bersifat sektoral seperti didalam Kitab Undang-Undang Hukum Pidana (KUHP). Penulis mengambil penelitian ini: 1) Untuk mengetahui pengaturan hukum pidana terhadap pemberantasan *cyber terorrism* dalam perspektif undang-undang nomor 19 tahun 2016 tentang informasi dan transaksi elektronik. 2) Untuk mengetahui dan menganalisis kebijakan hukum pidana yang

dapat dibangun dalam tindakan preventif cyber terrorism. Pendekatan Yuridis Normatif dilakukan untuk menjelaskan hukum yang tidak diperlukan dengan data-data dan/atau fakta-fakta sosial dalam perspektif Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang berkenaan dengan permasalahan penelitian ini. Hasil dan pembahasan menunjukan bahwa Pengaturan yang relatif terkait untuk menjerat pelaku terorisme siber di Indonesia saat ini ialah: 1). Pengaturan dalam UU ITE, 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.

Kata Kunci: *Cyber terrorism; UU ITE; Terorisme; Hukum Pidana*

1. Pendahuluan

Perkembangan teknologi informasi saat ini dapat dikatakan menimbulkan dua akibat yakni di satu sisi berakibat meningkatkan kesejahteraan dan kemajuan peradaban manusia dan di lain sisi berakibat juga menjadi sarana efektif perbuatan-perbuatan yang melawan hukum. [1] Hal inilah yang kemudian menjadi media atau sarana baru dalam tindakan terorisme, jika sebelumnya perbuatan terorisme dapat dilihat dan diketahui secara langsung hasil perbuatannya maka terorisme yang menggunakan internet sebagai sarana atau media melakukan aksi pergerakan kelompoknya menjadi lebih sulit untuk terdeteksi.

Dengan adanya perubahan paradigma aksi terorisme yang umumya dilakukan dengan menggunakan cara-cara yang konvensional namun saat ini hanya dengan menggunakan sebuah laptop atau komputer dengan bantuan internet mereka melakukan rangkaian aksi terorisme seperti halnya perekerutan anggota kelompok terorisme, melakukan aksi propaganda, melakukan pelatihan, pendanaan aksi terorisme yang mereka lakukan dengan maksud

[1] Ahmad Ramli, Cyber Law dan HAKI dalam sistem hukum Indonesia, Bandung, Rafika Adiama, 2004, hal. 1

dan tujuan untuk menyebarkan teror kepada masyarakat dan atau menunjukkan eksistensi kelompok mereka (cyber terrorism).

Jika kita melihat kasus-kasus terorisme yang telah terjadi di indonesia seiring berkembangnya teknologi informasi, kelompok teroris berhasil menggunakan kemudahan akses internet utuk melakukan serangkaian aksinya yang menimbulkan rasa takut di masyarakat, maka dapat diketahui bahwa kegiatan terorisme telah masuk ke dalam dunia cyber seperti halnya kasus pendanaan aksi terorisme yang dilakukan oleh Rizky Gunawan dengan cara hacking pada tahun 2010 yang digunakan untuk pembelian serta pelatihan aksi terorisme di poso. [2] selain itu, Kemudian, kasus cyber terrorism pertama di indonesia yang berhasil diungkap oleh Polri adalah kasus BOM Bali yang melibatkan terpidana mati Abdul Aziz alias imam Samudra pada 2002. Pada kasus ini, pelaku memang melakukan serangan secara nyata (fisik) yang mengakibatkan jatuhnya korban jiwa, kerusakan, dan kehancuran, tapi pelaku juga menggunakan jaringan internet sebagai media provokasi dan propaganda untuk mengintimidasi dan menakuti publik. Kasus ini menjadi rambu-rambu merah bagi Negara indonesia yang mensyaratkan bahwa ancaman cyber terrorism telah tampak secara nyata dan semakin dekat dengan kehidupan masyarakat.

Terkait dengan kejahatan di dalam dunia siber/cyber, indonesia telah mengaturnya di dalam Undang-Undang Nomor 11 tahun 2008 tentang informasi dan Transaksi elektronik sebagai langkah antisipasi atas pengaruh buruk dari pemanfaatan kemajuan teknologi iTe tersebut.[3]

---

[2] http://www.rmol.com Demi-Teroris,-Rizky-Gunawan-Sumbang-Ratusan-Juta-Hasil-Hacking, online diakses tanggal 2 Maret 2024

[3] Adami Chazawi, Ardi ferdian Tindak Pidana Informasi dan Transaksi Elektronik (penyerangan terhadap kepentingan hukum pemenfaatan teknologi informasi dan transaksi elektronik), Bayu Media, Malang. 2011, hal. 3

Undang-Undang ITE ini lebih menekankan pada tindak pidana cyber crime sebagai dasar perlindungan dari orang-orang yang mengancam hak orang atau masyarakat pengguna internet. Kejahatan dunia internet atau yang biasa disebut dengan cyber crime berbeda dengan kejahatan pada umumnya, perbedaan tersebut dapat dilihat pada karakteristik cyber crime yang diambil dari beberapa literatur yaitu : [4]

1. Perbuatan yang dilakukan secara ilegal tanpa hal atau tidak etis yang terjadi dalam ruang siber/cyber space.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan jaringan internet.
3. Perbuatan tersebut mengakibatkan kerugian materiil yang cenderung lebih besar dari kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya
5. Perbuatan tersebut sering dilakukan lintas Negara atau transnasional. Perbedaan mendasar dari cyber crime dan cyber terrorism terletak pada tujuan dan juga akibat yang ditimbulkan, jika cyber crime merupakan suatu bentuk kejahatan yang dilakukan dengan tujuan mencari keuntungan pribadi dan akibat yang ditimbulkan berupa kerugian kepentingan individu saja sedangkan cyber terrorism lebih kompleks yakni bertujuan untuk melakukan serangkain aksi terorisme yang dapat menimbulkan suasana teror kepada masyarakat luas.

Oleh karena itu pengaturan tentang tindak pidana *cyber terrorism* di indonesia untuk sementara ini belum secara jelas ada undang - undang yang mengatur secara khusus dan tidak jelasnya peraturan yang telah ada saat ini sehingga menimbulkan ketidakpastian hukum. Berdasarkan uraian diatas, penulis tertarik untuk mengkaji lebih mendalam lagi tentang bagaimana peranan kebijakan pemerintah menyikapi kasus cyber terrorism, melalui Penelitian skripsi yang berjudul **"**Analisis Yuridis Cyber Terrorism Dalam

[4] Abdul Wahid dan Mohammad Labib, Op Cit, hal. 76

Perspektif Undang-Undang Nomor 19 Tahun 2016 Tentang informasi Dan Transaksi elektronik**".**

2. Metode

Jenis Penelitian yang digunakan dalam penelitian ini adalah penelitian Hukum yuridis normatif. Penelitian hukum normatif adalah penelitian hukum kepustakaan yang mengacu pada norma hukum yang terdapat dalam peraturan internasional dan peraturan perundang-undangan. Penelitian ini juga dapat dikatakan sebagai penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder. Nama lain dari penelitian hukum normatif adalah penelitian hukum doktriner, juga disebut sebagai penelitian perpustakaan atau studi dokumen. Disebut penelitian hukum doktriner, karena penelitian ini dilakukan atau ditujukan hanya pada peraturan-peraturan yang tertulis atau bahan-bahan hukum yang lain. Sebagai penelitian perpustakaan ataupun studi dokumen disebabkan penelitian ini lebih banyak dilakukan terhadap data yang bersifat sekunder yang ada di perpustakaan. Termasuk dalam data sekunder meliputi buku-buku, buku-buku harian, surat-surat pribadi, dan dokumen-dokumen resmi dari pemerintah. Data sekunder ini dapat bersifat pribadi dan bersifat publik[5].

3. Pembahasan

3.1. Pengaturan Hukum Pidana Terhadap Pemberantasan *Cyber Terorrism* Dalam Perspektif Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik.

Secara umum terorisme dimaknai sebagai serangan terkoordinasi yang bertujuan membangkitkan perasaan teror terhadap sekelompok masyarakat.[6] Namun demikian, definisi terkait

[5] Bambang Waluyo, Penelitian Hukum Dalam Praktek, Ed. 1, Cet. 3, Sinar Grafika, Jakarta,2002, hal. 13-14.

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

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[7].

Cyber-terrorism merupakan konvergensi terorisme dan cyberspace[8]. Terorisme siber merupakan serangan teroris yang menggunakan peralatan jaringan komputer (cyberspace) untuk mengganggu sistem infrastruktur negara (energi, transportasi, operasional pemerintahan, dan sejenisnya) atau untuk

[7] 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, hal. 18

[8] 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, hal. 43

mengintimidasi pemerintahan atau sekelompok masyarakat sipil.[9] 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 UndangUndang Nomor 5 Tahun 2006 tentang Pengesahan international Convention for the Suppression of Terrorist Bombings.[10]

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.[11] Oleh

---

[9] 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 2 maret 2024

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

[11] Article VI, ASEAN Convention on Counter Terrorism: "The areas of cooperation under this Convention may, in conformity with the

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.[12]

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.[13] Dalam konteks itu, pengaturan yang relatif terkait untuk menjerat pelaku terorisme siber di indonesia saat ini ialah:

1). 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 teknologi informasi diantaranya, The United Nations Commissions

---

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, hal. 4

[12] Ibid

[13] Ibid, hal.5

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.[14] 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.

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 undangundang, seperti KUHP, UU iTe, dan UU Telekomunikasi. Ketiadaan aturan yang rinci mengenai terorisme siber ternyata juga berimplikasi pada peraturan 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.

[14] Barda N. Arief, Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia, Jakarta, PT. Raja Grafindo Persada, 2006, hal. 5

3.2. Kebijakan Hukum Pidana Yang Dapat Dibangun Dalam Tindakan Preventif Cyber Terrorism

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).[15] Kebijakan hukum pidana menurut Sudarto, bagaimana merumuskan hukum pidana yang baik yang akan diberlakukan dalam suatu waktu tertentu.[16] 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.[17]

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.[18] Kebijakan hukum pidana merupakan manifestasi dari segala usaha untuk merasionalkan hukum pidana dalam bentuk

---

[15] Salman Luthan, Kebijakan Kriminalisasi di Bidang Keuangan, Yogyakarta, FH UII Press, 2014, hal. 14

[16] Sudarto, Hukum Pidana dan Perkembangan Masyarakat: Kajian Terhadap Pembaharuan Hukum Pidana, Bandung, Sinar Baru, 1983, hal. 20

[17] Sudarto, Hukum dan Hukum Pidana, Bandung, Alumni, 2007, hal. 44-48

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

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). [19]

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).[20] Tahap kebijakan formulasi adalah tahap dihasilkannya suatu 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

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

[20] Ibid

melakukan reorientasi dan reformasi hukum pidana yang sesuai dengan nilainilai sentral sosiopolitik, sosiofilosofis, dan sosiokultural masyarakat indonesia.

A. 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.[21]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[22].

B. 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

[21] Barda N. Arief, Op. Cit., hal. 108
[22] Ibid

penegak hukum terhadap penanganan terorisme siber tersebut diharapkan dapat meminimalisir timbulnya konflik kewenangan antar lembaga.

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

D. 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.[23]

E. 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

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

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.

F. 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.

4. Kesimpulan

Pengaturan yang relatif terkait untuk menjerat pelaku terorisme siber di indonesia saat ini ialah: 1). Pengaturan dalam UU iTe, 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. Kebijakan Hukum Pidana Yang Dapat Dibangun Dalam Tindakan Preventif Cyber Terrorism yaitu upaya penal melalui kebijakan formulasi, upaya penal melalui kebijakan aplikasi, upaya penal melalui kebijakan eksekusi, upaya non-penal melalui pendekatan teknologi (techno prevention), upaya non-penal melalui peningkatan kerjasama antar negara (memory of

understanding), dan upaya non-penal melalui program deradikalisasi dunia maya.

Referensi

Buku:

Abdul Wahid dan Mohammad Labib, 2005*, Kejahatan Mayantara (Cyber Crime)*, PT. Refika Aditama, Jakarta.

Bahder Johan Nasution*, Metode Penelitian ilmu Hukum*, Mandar Maju, Bandung,2008.

Bambang Waluyo, *Penelitian Hukum Dalam Praktek*, ed. 1, Cet. 3, Sinar Grafika, Jakarta,2002.

Barda N. Arief, Sari Kuliah Perbandingan Hukum Pidana, PT. Raja Grafindo Persada, Jakarta, 2002.

edmom Makarim, *Pengantar Hukum Telematika*: Suatu Kompilasi Kajian (Jakarta: PT Raja Grafindo Persada, 2005).

irwansyah,*Penelitian Hukum*, Mirra Buana Media, Yogyakarta, 2021.

Judhariksawan, *Pengantar Hukum Telekomunikasi*, (Jakarta: Rajawali Press, 2005).

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

Sukawarsini Djelantik, Terorisme; Tinjauan Psiko-politis, Peran Media, kemiskinan, dan Keamanan Nasional, Jakarta, Yayasan Pustak Obor, 2010.

Wibowo, Ari, Hukum Pidana Terorisme (kebijakan formulatif hukum pidana dalam penanggulangan tindak pidana terorismedi indonesia), graham ilmu, yogyakarta, 2012.

Artikel Jurnal:

Nur Qalbi., Fitrah Marinda., dan Rina Yulianti. 2020. *Asean Against Cyber Terrorism: Upaya Mengatasi Propaganda Hitam sebagai Kejahatan Terorganisir*. Legislatif, Vol. 4.

Zephirinus Jondong. 2020. *Kebijakan Hukum Pidana bagi Tindak Pidana Cyber Terrorism dalam Rangka Pembentukan Hukum Positif di indonesia*., Jurnal Preverensi Hukum., Vol.1., No. 2

Alfendo Yefta Argastya, Supanto.2022. *Penerapan Hukum Pidana Pada Penyidikan Kepolisian Untuk Menanggulangi Kejahatan Cyber-Terrorism*. Recidive. Volume 11 issue 1.

Petrus Reinhard Golose, *Perkembangan Cyber Crime dan Upaya Penanggulangannya di indonesia oleh Polri*, Buletin Hukum Perbankan dan Kebanksentralan, Volume 4 Nomor 2, Agustus 2006.

Peter Stephenson, 2000, *investigating Computer-Related Crime: A Handbook For Corporate investigators*, CRC Press, London-New York-Washington D.C.

Hafidz Putera Nugraha, *Analisis yuridis rumusan delik tentang tindak pidana cyber terrorism ditinjau dari undang-undang nomor 15 tahun 2003 tentang pemberantasan tindak pidana terorisme dan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.* Skripsi Sarjana Hukum Universitas Sebelas Maret Surakarta,Surakarta,2011

Peraturan Perundang-Undangan:

Undang-Undang Nomor 19 Tahun 2016 tentang informasi dan Transaksi elektronik

Undang-Undang Republik indonesia Nomor 9 Tahun 2013 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme

Website:

http://tekno.kompas.com/read/2017/05/13/17180077 (diakses 28 oktober 2023).

https://paralegal.id/pengertian/informasi-elektronik/ (diakses tanggal 31 Januari 2024)

https://sippn.menpan.go.id/berita/58352/ (diakses tanggal 29 oktober 2023).

https://jdih.ppatk.go.id/produk-hukum (diakses tanggal 29 oktober 2023)

http://www.pengertianartidefinisi.compengertian-hukum-yuridis (diakses pada tanggal, 29 Maret, 2024

Pengertian Tinjuan Yuridis_http://infopengertian.biz/pengertian-yuridis-da-penerapa nnya-di-masyarakat.html, Kabanjahe, diakses pada tanggal 18 Desember 2021