RECIDIVE
JURNAL HUKUM PIDANA DAN PENANGGULANGAN KEJAHATAN

Volume 11 Issue 1, 2022
E-ISSN: 2775-2038
This work is licensed under a Creative Commons Attribution 4.0 International License

PENERAPAN HUKUM PIDANA PADA PENYIDIKAN KEPOLISIAN UNTUK MENANGGULANGI KEJAHATAN *CYBER-TERRORISM*

Alfendo Yefta Argastya[1], Supanto[2]

[1,2]Fakultas Hukum, Universitas Sebelas Maret
Email: [1]alfendoyefta02@gmail.com, [2]supanto.8787@gmail.com

Abstrak: Penelitian ini bertujuan untuk mengetahui pengaturan hukum pidana dalam mengakomodasi kejahatan cyber-terrorism di Indonesia serta penerapan hukum pidana yang dilakukan kepolisian dalam proses penyidikan untuk menangani kejahatan cyber-terrorism. Penelitian ini merupakan penelitian hukum normatif, bersifat perspektif dengan menggunakan bahan hukum primer maupun sekunder yang dianalisis dengan metode penalaran logika deduktif. Teknik pengumpulan bahan hukum yang digunakan adalah studi kepustakaan. Untuk penunjang bahan hukum, dilakukan wawancara dengan pihak Subdit V/Siber Direktorat Reserse Kriminal Khusus Polda Jawa Tengah. Hasil penelitian diperoleh bahwa tindak pidana cyber-terrorism belum dirumuskan ke dalam peraturan perundang- undangan. Dalam mengantisipasi tindak pidana cyber-terrorism penyidik menggunakan instrumen hukum UU ITE dan UU Terorisme. Dalam penelitian ini juga dilakukan inventarisasi instrumen hukum yakni KUHP, UU Pendanaan Terorisme, dan UU Telekomunikasi. Tetapi instrumen tersebut tidak bisa diterapkan pada tindak pidana cyber-terrorism. Penyidik dalam melakukan penyidikan terhadap tindak pidana cyber-terrorism menggunakan instrumen hukum UU ITE dan UU Terorisme dalam jangka waktu sementara.

Kata Kunci: Cyber-terrorism, Penyidikan, Pengaturan Hukum Pidana, Penerapan Hukum Pidana oleh Penyidik.

Abstract: This research aims to determine the regulation of criminal law in accommodating cyber-terrorism crimes in Indonesia and the application of criminal law by the police in the investigation process to deal with cyber-terrorism crimes. This research is a normative legal research, with a perspective using primary and secondary legal materials which are analyzed using deductive logic reasoning methods. The technique of collecting legal materials used is literature study. To support legal material, interviews were conducted with the SubDirectorate V/Siber of the Directorate of Special Criminal Investigation at the Central Java Police. The results showed that the crime of cyber-terrorism has not been formulated into legislation. In anticipating criminal acts of cyber-terrorism, investigators use the legal instruments of the ITE Law and the Terrorism Law. In this study, an inventory of legal instruments was also carried out, namely the Criminal Code, the Terrorism Financing Act, and the Telecommunications Law. However, this instrument cannot be applied to criminal acts of cyber-terrorism. Investigators in conducting investigations into criminal acts of cyber-terrorism use the legal instruments of the ITE Law and the Terrorism Law for a temporary period.

Keywords: Cyber-terrorism, Investigation, Criminal Law Regulation, Application of Criminal Law by Investigators.

1. Pendahuluan

Akses informasi menjadi sangat mudah sebagai konsekuensi dari kemajuan ilmu pengetahuan dan teknologi, terutama telekomunikasi yang sudah membuat masyarakat tidak memiliki batasan ruang dalam melakukan komunikasi (Aris Hardinanto 2019:1). Perkembangan teknologi pada prinsipnya memegang peranan penting dalam mengonstruksi dinamika kehidupan manusia, karena diperhitungkan sebagai unsur yang dapat berandil dalam kehidupan manusia. Terlebih, pemanfaatan teknologi saat ini juga merambah di bidang hukum. Hal tersebut sejalan dengan pemikiran hukum progresif yang dicetuskan oleh Satjipto Rahardjo, di mana hukum hendaknya mampu mengikuti perkembangan zaman, mampu menjawab perubahan zaman dengan segala dasar di dalamnya, serta mampu melayani masyarakat dengan menyandarkan pada aspek moralitas dan kemampuan dari sumber daya manusia penegak hukum itu sendiri (Satjipto Raharjo 2006:11).

Tidak dapat dipungkiri bahawasanya disamping kemanfaatan yang diperoleh, perkembangan teknologi dan informasi juga menjadi salah satu penyumbang terbanyak modus dan motif kejahatan yang ada di dalam masyarakat, yakni dengan memanfaatkan komputer sebagai sarana untuk melakukan sebuah kejahatan. Penyalahgunaan komputer ini banyak menimbulkan permasalahan yang sangat kompleks khususnya dalam proses penegakan hukum, mengingat komputer sebagai salah satu media yang memiliki karakteristik tersendiri yang sangat bertolak belakang dengan media yang sering digunakan dalam melakukan kejahatan-kejahatan secara konvensional (Sheila Maulida Fitri 2020:2).

Kemudahan dalam membagikan sekaligus menerima informasi melalui jaringan nirkabel pada era digital dipandang menarik para pelaku kejahatan untuk melancarkan tindakan yang dilarang oleh hukum. Pelaku kejahatan siber (cybercrime) bisa dengan mudah melakukan tindakan yang merugikan korban, hal tersebut karena korban 2 kejahatan siber (cybercrime) tidak bisa melihat tindakan atau perbuatan pelaku kecuali korban juga terkoneksi dengan internet. Berbicara mengenai kejahatan siber (cybercrime) sudah barang tentu ada kaitannya dengan tindak pidana. Moeljatno memberikan definisi tindak pidana sebagai perbuatan yang dilarang oleh suatu aturan hukum, di mana larangan tersebut disertai sanksi berupa pidana tertentu bagi siapapun yang melanggar aturan (Moeljatno 2015:60). Perkembangan teknologi yang pesat memberikan pengaruh pada perkembangan jenis tindak pidana baru yang lebih mutakhir yang salah satunya adalah tindak pidana siber. Tindak pidana siber adalah implikasi dari munculnya aktivitas yang masif di ruang siber yang biasa dikenal dengan cyberspace. Perkembangan tindak pidana siber yang masih sangat relatif baru mengakibatkan belum adanya pengertian yang final terhadap kejahatan siber (cybercrime) itu sendiri.

Indonesia pernah mengalami serangan cyber-terrorism tepatnya pada bulan Mei 2017 lalu, terdapat dua rumah sakit yaitu Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais. Menurut Dirjen Aplikasi Informatika, Samuel mengatakan serangan ini memiliki sifat masif serta menyasar critical resource (sumber daya yang sangat penting). Serangan ini mengakibatkan gangguan pada sistem komputer yang berkaitan dengan proses administrasi rumah sakit sehingga menyulitkan pelayanan medis bagi pasien. Serangan cyber-terrorism ini menginfeksi semua komputer yang terkoneksi dengan internet. Kemudian serangan siber ini berjenis ransomeware wannacry. Di lihat dari

tampilan komputer diketahui ransomeware ini meminta dana tebusan yang diminta dengan pembayaran melalui bitcoin.

Cyber-terrorism menjadi ancaman yang sangat serius dan membutuhkan pencegahan secara komperhensif oleh pemerintah. Mengapa demikian, karena serangan cyber-terrorism ini bisa menyerang apa saja yang terhubung dengan internet terlebih menyerang objek vital negara yang bisa menganggu fungsi bahkan dapat menimbulkan korban yang jauh lebih besar daripada aksi terorisme yang dilakukan secara konvensional. Aturan hukum yang mengatur mengenai tindak pidana cyber-terrorism di Indonesia sampai saat ini belum menemui kejelasan dan kepastian (Agis Josianto Adam 2014:165). Namun rupa-rupanya perlu adanya pemberian batasan definisi tindak pidana cyber-terrorism guna menunjukkan benang merah antara terorisme siber dengan definisi terorisme itu sendiri. Hal tersebut guna menentukan aturan hukum mana yang paling tepat diterapkan dalam melakukan penegakan hukum atas serangan cyber-terrorism di Indonesia.

Jika melihat aturan lain yang ada sedikit kaitannya dengan kejahatan cyber-terrorism yakni Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (selanjutnya disebut UU ITE) dan Undang- Undang Republik Indonesia Nomor 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang (selanjutnya disebut UU Terorisme). Kedua aturan tersebut masih menimbulkan kerancuan dan menghambat kinerja aparat jika terjadi serangan cyber-terrorism. Gustav Radbruch mengatakan ada 3 (tiga) tujuan hukum yang salah satunya adalah kepastian hukum yang artinya aparat dalam melakukan penegakan hukum harus berlandaskan aturan yang jelas. Oleh sebab itu, penulis tertarik untuk meneliti pengaturan hukum pidana terkait untuk menangani kejahatan cyber-terrorism dan bagaimana proses penegakan hukumnya. Kemudian penulis juga akan menguraikan instrumen hukum lain yang memiliki keterkaitan dengan tindak pidana cyber-terrorism.

2. Rumusan Masalah

Berdasarkan uraian latar belakang tersebut di atas, penelitian ini akan mengkaji lebih lanjut mengenai bagaimana pengaturan hukum pidana dalam mengantisipasi kejahatan cyber-terrorism di Indonesia dan bagaimana penerapan hukum pidana yang dilakukan kepolisian dalam proses penyidikan untuk menangani kejahatan cyber-terrorism.

3. Metode Penelitian

Jenis penelitian yang digunakan penulis dalam penelitian ini merupakan penelitian hukum normatif atau sering disebut sebagai penelitian hukum doktrinal. Penelitian hukum normatif adalah penelitian berdasarkan pada bahan-bahan hukum primer dan sekunder yang nantinya dapat menghasilkan argumentasi teori, dan konsep baru sebagai penyelesaian masalah yang dihadapi (Peter Mahmud Marzuki, 2014: 60). Sifat penelitian yang digunakan dalam penelitian ini adalah bersifat preskriptif dan terapan. Preskriptif

adalah mempelajari tujuan hukum, nilai-nilai keadilan, validasi aturan hukum, konsep hukum, dan norma hukum. Penelitian preskriptif bertujuan untuk memberikan gambaran atau merumuskan masalahsesuai dengan keadaan atau fakta yang ada. Pendekatan yang digunakan penulis dalam penelitian ini adalah pendekatan perundang-undangan (statute approach), pendekatan kasus (case approach) dan pendekatan konseptual (conceptual approach).

Sumber bahan hukum yang penulis gunakan yaitu bahan hukum primer berupa Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan Atas Undang- Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang, Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi, Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme, Kitab Undang-Undang Hukum Pidana (KUHP). Bahan hukum sekunder berupa hasil penelitian, tulisan-tulisan karya ilmiah, jurnal, kamus- kamus hukum, dan hasil wawancara yang secara tidak langsung memberikan keterangan terkait bahan hukum primer dan mampu mendukung penelitian ini.

Metode pengumpulan data yang digunakan penulis dalam penelitian ini adalah studi kepustakaan (library research). Pengumpulan data yang dilakukan menggunakan cara menganalisis suatu konten yang berkaitan. Teknik ini digunakan untuk mendapatkan landasan teori dengan mengkaji dan mempelajari buku, peraturan perundang-undangan, dokumen, arsip, laporan, dan hasil penelitian yang serupa atau saling berkaitan dengan masalah yang diteliti (Peter Mahmud Marzuki, 2014: 273).

4. Pembahasan

4.1. Pengaturan Hukum Pidana Dalam Mengantisipasi Kejahatan Cyber- terrorism di Indonesia

Perlu diketahui kembali bahwa kejahatan siber pada hakikatnya merupakan bentuk kejahatan yang ditujukan terhadap komputer dan jaringannya. Hal tersebut merupakan konsekuensi dari pesatnya perkembangan teknologi yang hampir merambah di berbagai sektor krusial. Selama 20 tahun terakhir, teknologi informasi berkembang sangat signifikan. Dari mulai alat administrasi dalam rangka mengoptimalkan proses kantor, sekarang menjadi instrumen strategis industri, pemerintahan bahkan militer (Constantin & Monica 2015:115). Namun pesatnya teknologi tersebut memiliki celah yang sangat rawan dan berbahaya. Bahwa dalam ruang maya (cyberspace) memiliki atau terdapat kerentanan yang sangat serius sehingga berpotensi terjadi sebuah kejahatan. Seperti halnya terorisme, tindak kejahatan terorisme sendiri mengalami perkembangan sangat pesat yang awalnya dilakukan secara konvensional sekarang berubah menjadi modern dengan memanfaatkan internet untuk melakukan aksi kejahatan.

Cyberspace dapat dikatakan sebagai tempat untuk para teroris melancarkan aksinya seperti melakukan hacking atau pemerasan (ransomeware) guna memperoleh dana yang digunakan untuk membiayai aksi terornya. Selain itu, teroris menggunakan media teknologi informasi untuk saling melakukan komunikasi serta berkoordinasi dalam rangka memperiapkan

agenda mereka. Pada hakikatnya terorisme siber (cyber- terrorism) merupakan tindak kejahatan melawan hukum yang direncanakan oleh seseorang atau kelompok dengan motif politis untuk mencapai ideologinya, yang dilakukan baik langsung maupun tidak langsung dengan cara melakukan serangan, merusak data informasi, sistem komputer, bahkan program komputer (Zephirinus Jondong 2020:22). Terlebih pelaku cyber-terrorism ini menyerang terhadap instalasi penting yang dimiliki negara sehingga menimbulkan kekacauan dan menebar rasa takut dengan menggunakan sarana internet sebagai instrumen melakukan kejahatan.

Berkaitan dengan instrumen hukum yang mengatur mengenai tindak pidana cyber-terrorism secara experssive verbist belum diatur dalam sebuah peraturan perundang-undangan sehingga hal tersebut menimbulkan problematika dan ketidakpastian dalam upayanya mengakomodir tindak kejahatan cyber-terrorism. Jika tindak pidana cyber-terrorism terjadi, lantas aparat penegak hukum harus menggunakan dasar hukum apa untuk menangani kejahatan tersebut. Mengingat dalam hukum pidana ada istilah asas legalitas. Asas legalitas disini mengandung arti bahwa jika ingin menjerat suatu perbuatan maka harus ada aturan hukum yang mengatur terlebih dahulu namun apabila tidak ada regulasi yang mengatur maka perbuatan tersebut tidak dapat dipidana. Padahal tindak pidana cyber-terrorism ini sangat berbahaya dan harus di waspadai.

Dalam mengakomodir tindak pidana cyber-terrorism di Indonesia, penulis mencoba meninjau menggunakan instrumen hukum yang ada yakni dengan melihat Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor I1 Tahun 2008 tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang serta peraturan lain sepanjang ada keterkaitan dengan tindak pidana cyber-terrorism. Rupa-rupanya jika melihat aturan tersebut maka sudah barang tentu wajib untuk dibedah betul guna menentukan pasal untuk menjerat tindak pidana cyber-terrorism.

a) Pengaturan Kejahatan Cyber-terrorism di Dalam Kitab Undang- Undang Hukum Pidana (KUHP)

Suatu hal yang harus dipahami adalah hukum pidana saat ini yang disampaikan oleh Jan Remmelink dalam setiap delik apa yang berfungsi dan dianggap sebagai unsur pembentuk selain perilaku manusia juga berbuat dan tidak berbuat, sikap batin seseorang betapapun immoral ataupun tercelanya bagi masyarakat, tidaklah penting. Saat ini hukum pidana masih terfokus pada tindakan. Dalam hal ini, bukan saja kualifikasi individu yang berbahaya secara sosial yang menjadi fokus utama, tetapi juga perbuatan yang dilakukan (Arief dalam Ahmad Faizal 2020:276). Kemudian dalam kaitannya perkembangan kejahatan dunia maya tentu jika menelaah Kitab Undang-Undang Hukum Pidana (KUHP), dinilai tidak lengkap dan tidak lagi dapat mengakomodir masalah hukum yang berdimensi tindak pidana baru, karena kurang sesuai dengan nilai sosio-filosofik, sosio-politik dan sosio-kultural yang hidup di masyarakat (Barda Nawawi 2011:14).

Rumusan delik dalam KUHP masih bersifat konvensional dan sama sekali belum mengatur mengenai jenis tindak pidana siber yang salah satunya adalah cyber-terrorism.

Beberapa pasal dalam KUHP dapat dikorelasikan dengan tindak pidana terorisme siber namun terkendala dalam penerapannya yaitu ketentuan sebagai berikut:

No	Pasal	Keterangan
1.	Pasal 168 ayat (1), (2), dan (3)	Kejahatan terhadap ketertiban Umum
2.	Pasal 340	Kejahatan terhadap nyawa
3.	Pasal 362	Pencurian
4.	Pasal 368	Pemerasan dan Pengancaman

Tabel 1. Pengaturan KUHP Jika Dikaitkan Dengan Cyber-terrorism

Berdasarkan pasal-pasal di atas jika dirunut berdasarkan unsurnya maka sudah sangat jelas bahwa rumusan bentuk tindak pidananya masih bersifat konvensional sehingga tidak memenuhi kualifikasi kejahatan cyber- terrorism. Untuk lebih meyakinkan lagi perlu adanya penjelasan mengenai kejahatan cyber-terrorism guna menguji pasal-pasal tersebut. Bahwa serangan siber dilakukan dalam ruang maya yang bermotif kanpolitik yang berpotensi mengakibatkan kematian. Kemudian serangan siber menyebabkan ketakutan dan merugikan baik materiil atau immateriil. Yang paling penting adalah kejahatan cyber-terrorism menyerang objek vital negara. Menurut hemat penulis, maka pasal-pasal tersebut tidak relevan dengan kejahatan cyber-terrorism.

b) Pengaturan Kejahatan Cyber-terrorism di Dalam Undang-Undang Telekomunikasi

Dalam rangka penegakan hukum untuk mengantisipasi tindak pidana cyber-terrorism, penulis mencoba mengkaji masalah ini dengan Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi) dikaitkan dengan tindak pidana cyber-terrorism. Berangkat dari permasalahan tersebut, telematika sangat berkorelasi dengan hajat hidup orang banyak, karena di dalamnya terdapat sumber daya terbatas sebagai contoh frekuensi radio dan pengaturannya secara terkoordinatif, interkoneksi antar penyelenggara dan antar regional. Dalam penjelasan umum UU Telekomunikasi disebutkan bahwasanya Perubahan lingkungan global dan perkembangan teknologi telekomunikasi yang berlangsung sangat cepat telah mendorong terjadinya perubahan mendasar, melahirkan lingkungan telekomunikasi yang baru, dan perubahan cara pandang dalam penyelenggaraan telekomunikasi, termasuk hasil konvergensi dengan teknologi informasi dan penyiaran, sehingga dipandang perlu mengadakan penataan kembali penyelenggaraan telekomunikasi nasional.

Percepatan tersebut juga menimbulkan sisi-sisi negatif yakni berkembangnya ancaman dan gangguan yang dilakukan menggunakan media telekomunikasi. Kaitannya dengan tindak pidana cyber-terrorism, penulis memfokuskan pada Pasal 21 UU Telekomunikasi yang diberbunyi:

"Penyelenggara telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, keamanan atau ketertiban umum".

Berdasarkan bunyi pasal di atas, menurut hemat penulis Pasal 21 UU Telekomunikasi hanya menyatakan perbuatan yang dilarang yakni kepentingan umum, kesusilaan, keamanan atau ketertiban umum. Kemudian kaitannya dengan tindak pidana cyber-terrorism penulis mengerucutkan pada frasa keamanan dan ketertiban umum. Tafsir frasa tersebut masih sangat luas dalam Pasal 21 UU Telekomunukasi tersebut. Dasar argumentasinya adalah pada Pasal tersebut tidak dijelaskan secara detail mengenai frasa keamanan dan ketertiban umum yang seperti apa dalam UU Telekomunikasi. Kaitannya dengan tindak pidana cyber-terrorism, memang tindak pidana tersebut mengancam keamanan dan ketertiban umum, tetapi dalam pasal tersebut belum dapat diterapkan pada tindak pidana cyber-terrorrism karena tafsir yang sangat luas dan UU Telekomunikasi sendiri diperuntukan hanya untuk mengtur jalannya komunikasi antar penyelenggara. Selain itu definisi telekomunikasi sendiri adalah berdasarkan Pasal 1 angka 1 yang berbunyi:

"Telekomunikasi adalah setiap pemancaran, pengiriman dan atau penerimaan dari hasil informasi dalam bentuk tanda- tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya".

Mengingat tindak pidana cyber-terrorism dalam melakukan aktivitasnya dengan menggunakan instrumen jaringan internet dan menyerang komputer yang menyasar kepada objek vital negara.

c) Pengaturan Kejahatan Cyber-terrorism di Dalam Undang-Undang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme.

Dasar dibentuknya Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme (UU Pendanaan Terorisme) ini bukan hanya karena keresahan terhadap banyaknya ancaman bom atau bentuk terorisme lainnya yang sering terjadi, melainkan untuk memberikan kepastian hukum dalam suatu hukum positif guna mengatur upaya pencegahan dan pemberantasan tindak pidana pendanaan terorisme di Indonesia. Selama ini pendekatan yang digunakan oleh aparat penegak hukum dengan mendasarkan pada UU Terorisme masih terbatas pada upaya mengejar pelaku sehingga dapat dijatuhi hukuman sesuai dengan peraturan perundang-undangan. Tentu pendekatan follow the supect tidak membuat perbuatan atau kegiatan teror berhenti. Dengan jaringan yang begitu luas dan tersembunyi membuat eksistensi mereka tetap terjaga.

Berkaitan dengan tindak pidana cyber-terrorism dalam UU Pendanaan Terorisme, menurut hemat penulis tidak diatur sama sekali mengenai tindak pidana tersebut. Dalam UU a quo hanya mengatur sebatas transaksinya saja. Dasar argumentasinya adalah jika berbicara mengenai pendanaan terorisme maka merujuk pada Pasal 1 angka 1 yang berbunyi:

"Pendanaan Terorisme adalah segala perbuatan dalam rangka menyediakan, mengumpulkan, memberikan, atau meminjamkan Dana, baik langsung maupun tidak

langsung, dengan maksud untuk digunakan dan/atau yang diketahui akan digunakan untuk melakukan kegiatan terorisme, organisasi teroris, atau teroris".
Kemudian definisi transaksi dalam Pasal 1 angka 5 yang berbunyi:
"Transaksi adalah seluruh kegiatan yang menimbulkan hak dan/atau kewajiban atau menyebabkan timbulnya hubungan hukum antara dua pihak atau lebih".

Maka hal tersebut sudah jelas dalam UU ini hanya sebatas transaksinya saja, kendatipun transaksi menggunakan sarana internet sebagai contoh i-banking, payment, dan mobile banking maka UU Pendanaan Terorisme ini tidak dapat diterapkan pada tindak pidana cyber-terrorism. Kemudian jika menggunakan media internet untuk melakukan pendanaan terorisme dengan cara membobol dana masyarakat melalui peretasan (hacking) situs investasi online untuk dimodifikasi nilai investasinya kemudian investasi tersebut dijual untuk mendapatkan uang, maka tindakan tersebut dapat dijerat dengan UU ITE bukan dengan UU Pendanaan Terorisme. Karena modus daripada tindak pidana cyber-terrorism ini memiliki sifat menyerang dengan memanfaatkan instrumen jaringan untuk mendapatkan apa yang diinginkan. Dan biasanya dalam kasus tindak pidana cyber-terrorism dalam melakukan aksinya dengan menyerang komputer sehingga komputer menjadi terganggu dan meminta uang tebusan supaya komputer bisa diakses kembali yang selanjutnya pelaku meminta tebusan uang dalam bentuk bitcoin.

d) Pengaturan Kejahatan Cyber-terrorism di Dalam Undang-Undang Informasi dan Transaksi Elektronik

Terkait perkembangan kejahatan terorisme di dunia maya maka diperlukan instrumen hukum untuk mengatur hal tersebut. UU ITE sebagai peraturan yang bersifat administratif tidak luput mengatur cakupan hukum yang dimungkinkan dapat terjadi sebagai dampak negatif adanya penyalahgunaan teknologi. Hal ini dengan pertimbangan untuk melindungi kepentingan bangsa Indonesia mengingat pemanfaatan teknologi bersifat lintas teritorial. Pihak manapun bahkan di seluruh dunia dapat melakukan aktivitas yang berkaitan dengan informasi dan transaksi elektronik yang kemudian juga memiliki implikasi hukum di Indonesia atau merugikan kepentingan Indonesia, maka pihak tersebut dapat terjerat UU ITE. Dalam penjelasan UU ITE disebutkan bahwa "merugikan kepentingan Indonesia" adalah perbuatan yang dapat mengakibatkan adanya kerugian terhadap kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara. Dalam konsideran UU ITE berkembangnya teknologi menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah mempengaruhi lahirnya bentuk-bentuk kejahatan baru termasuk salah satunya cyber-terrorism.

Kaitannya dengan penegakan hukum terkhusus pada proses penyidikan penulis memfokuskan pada 3 (tiga) pasal, yakni Pasal 30, Pasal 32, dan Pasal 33 UU ITE. ketentuan Pasal 30 dan Pasal 32 sesungguhnya memiliki dimensi pengaturan yang dapat mengakomodir kejahatan cyber-terrorism dengan sanksi sebagaimana yang diatur dalam Pasal 46 dan Pasal 48 dengan ancaman hukuman penjara maksimal 10 tahun dan denda maksimal Rp. 5.000.000.000, -. (lima miliar rupiah). Namun rumusan delik dalam kedua Pasal tersebut dinilai masih sangat sederhana sehingga lebih tepat ditegakan terhadap terorisme siber yang menyerang individu atau perseorangan, bukan terhadap serangan yang masif.

Frasa masif dalam hal ini bersifat sangat meluas yang artinya perbuatan tersebut menyerang instalasi penting negara dan fasilitas publik sehingga berdampak di berbagai sektor dan lini masyarakat.

Menelaah Pasal 30 UU ITE, dalam konstruksi pasal tersebut mengatur mengenai tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun. Perbuatan dalam rumusan pasal tersebut menerangkan bahwa tindakan illegal yang dilakukan seseorang terhadap sistem elektronik milik orang lain dengan tujuan untuk memperoleh informasi dokumen elektronik dan/upayanya penerobosan, pembobolan, dan penjebolan yang melanggar melampaui batas sistem keamanan. Sedangkan dalam Pasal 32 dan Pasal 33 UU ITE dalam konstruksinya mengatur perlindungan terhadap suatu informasi dan/atau dokumen elektronik baik milik orang lain atau milik publik yang memiliki sifat rahasia. Dalam rumusan Pasal tersebut terdapat frasa melawan hukum. Melawan hukum (wederrechtelijkheid) sendiri dalam doktrin hukum pidana berdasarkan Memorie van Toelichting atau sejarah pembentukan KUHP di Belanda tidak ditemukan apakah yang dimaksudkan dengan kata "hukum" dalam frasa "melawan hukum". Jika merujuk pada postulat contra legem facit qui id facit quod lex prohibit; in fraudem vero qui, salvis verbis legis, sententinam ejus circumuenit, maka dapat diartikan bahwa seseorang dinyatakan melawan hukum ketika perbuatan yang dilakukan adalah suatu perbuatan yang dilarang oleh hukum (Eddy O.S Hiariej 2016:232).

Kaitannya dengan sifat melawan hukum dalam konstruksi Pasal 30 UU ITE tersebut mempunyai dua corak, yakni melawan hukum objektif dan melawan hukum subjektif. Unsur objektif disini dimaksudkan unsur yang berhubungan dengan keadaan, artinya di dalam keadaan mana tindakan pelaku itu harus dilakukan. Sedangkan unsur subjektif adalah unsur yang melekat pada diri pelaku atau yang berhubungan dengan diri pelaku (Anselmus S. J. Mandagie 2020:53). Jika dikaitkan dengan konstruksi pasal tersebut unsur objektif berarti komputer dan/atau sistem komputer tersebut bukan milik pelaku serta perbuatan akses komputer atau sistem elektronik tersebut illegal dan dalam konteks subjektif pelaku memiliki niat jahat untuk mengakses komputer secara illegal.

Kemudian seperti halnya Pasal 30 UU ITE, Pasal 32 UU ITE juga memiliki dua corak melawan hukum yakni objektif dan subjektif. Objektif dalam konstruksi pasal 32 terdapat pada unsur objeknya yakni informasi elektronik dan dokumen elektronik tersebut milik orang lain. Agar rumusan tersebut memenuhi sifat melawan hukum objektif, maka frasa milik orang lain tersebut wajib dan harus dibuktikan keberadaannya melalui perbuatan mengubah harus tidak ada izin dari pemiliknya. Lalu sifat melawan hukum yang subjektif bertumpu pada keadaan/sikap batin pelaku terhadap sifat melawan hukum objektif. Selanjutnya dalam Pasal 33 UU ITE pada hakikatnya sifat melawan hukum terletak pada materiil/ akibat tindakan tersebut, yakni tindakan pelaku akan berimplikasi terganggunya sistem elektronik (Zephirinus 2020:24)

Konstruksi Pasal 30, 32, dan 33 UU ITE pada intinya dapat diterapkan dalam kerangka penegakan hukum untuk mempidana pelaku kejahatan cyber-terrorism. Ketiga pasal tersebutlah yang mendekati cara kerja pada kejahatan cyber-terrorism, yakni mengakses komputer tanpa izin, mengubah, merusak dokumen elektronik yang tersimpan, dan melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem

elektronik, terlebih pelaku memasuki sistem jaringan komputer dan mengenskripsi data sehingga tidak dapat diakses kembali bahkan pelaku juga melakukan pemerasan dengan meminta uang.

Namun konstruksi pasal tersebut memiliki kekurangan yakni lebih mengarah pada tindak pidana yang dilakukan terhadap individu. Mengingat kembali bahwasanya kejahatan cyber- terrorism memiliki sifat serangan yang masif. Kemudian sifat melawan hukum untuk konteks kejahatan cyber-terrorisme tidak terpenuhi dalam konstruksi pasal-pasal UU ITE karena dalam tindak pidana cyber-terrorism ancaman dan serangan secara melawan hukum dilakukan hanya terhadap komputer, data, dan jaringan yang tersimpan, lalu memiliki tujuan untuk melakukan intimidasi terhadap pemerintah bahkan masyarakat untuk tujuan politik atau sosial tertentu. Intimidasi disini dimaksudkan dengan menebar ketakutan atau teror yang akan menganggu stabilitas keamanan negara.

e) Pengaturan Kejahatan Cyber-terrorism di Dalam Undang-Undang PemberantasanTindak Pidana Terorisme

Berbicara mengenai pengaturan tindak pidana cyber- terrorism, penulis memfokuskan pada Pasal 6 UU Terorisme yang berbunyi:

"Setiap Orang yang dengan sengaja menggunakan Kekerasan atau Ancaman Kekerasan yang menimbulkan suasana teror atau rasa takut terhadap orang secara meluas, menimbulkan korban yang bersifat massal dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran terhadap Objek Vital yang Strategis, lingkungan hidup atau Fasilitas Publik atau fasilitas internasional dipidana dengan pidana penjara paling singkat 5 (lima) tahun dan paling lama 20 (dua puluh) tahun, pidana penjara seumur hidup, atau pidana mati".

Berdasarkan pasal yang sudah diuraikan di atas, menurut hemat penulis pasal tersebut mendekati dengan bentuk kejahatan cyber-terrorism. Itu pun terletak pada frasa ancaman kekerasan yang menimbulkan suasana teror atau rasa takut terhadap orang secara meluas serta menimbulkan korban yang bersifat masal. Serangan cyber-terrorism harus berimplikasi pada orang atau barang atau setidaknya cukup menyebabkan ancaman bahaya untuk menimbulkan rasa takut. Sebab, kendatipun dilakukan dalam suatu sistem elektronik, serangan cyber-terrorism ini tetap terdiri dari unsur-unsur yang terdapat dalam terorisme konvensional (Janet dkk 2004:280). Unsur-unsur yang terdapat dalam terorisme konvensional, yakni: adanya kerusakan, ketidakpastian, ketakutan, keputusasaan bahkan kematian. Kemudian dalam tindak pidana cyber-terrorism harus dilihat terlebih dahulu identitas pelaku, motivasi, dan tujuan yang dilakukannya, serta akibatnya (Varvara 2001:5).

Namun kekurangan dan celah dari Pasal 6 UU Terorisme ini adalah bahwa dalam rumusannya tidak dijelaskan menggunakan instrumen apa pelaku teror melakukan aksinya, bahwa cyber- terrorism ini menggunakan sarana internet dan jaringan untuk setiap kegiatannya. Ini tentunya harus menjadi perhatian serius karena modus dan bentuk kejahatan terkhusus terorisme terus mengalami progres perkembangan yang signifikan.

f) Cakupan Pengaturan Hukum Pidana Terhadap Kejahatan Cyber- terrorism dalam UU ITE dan UU Terorisme

Setelah menguraikan dan menginventarisasi pasal-pasal yang terdapat dalam beberapa undang-undang yang kemudian penulis kerucutkan hanya 2 undang-undang saja yakni UU

ITE dan UU Terorisme, lalu penulis akan mengkorelasikan antara unsur- unsur yang terdapat dalam UU ITE dan UU Terorisme sebagai cakupan pengaturan hukum pidana terhadap kejahatan cyber- terrorism. Berdasarkan cakupan unsur-unsur pasal di dalam UU ITE dan UU Terorisme yang kemudian dikorelasikan menunjukkan bahwa sesungguhnhya tindakan serta akibat yang ditimbulkan dalam serangan cyber-terrorism telah memenuhi unsur sebagaimana yang diatur dalam kedua instrumen hukum tersebut. Namun dalam perspektif UU Terorisme jika ditinjau dari sikap batin atau motifnya, serangan cyber-terrorism yang masif, menyerang objek vital sehingga menimbulkan suasana teror yang meluas tidak masuk dalam tindak pidana terorisme karena tindak memenuhi kualifikasi motif politik dan ideologi meskipun sesungguhnya sama-sama menimbulkan gangguan keamanan. Indikator penentu suatu tindakan dapat dikategorikan sebagai tindak pidana terorisme sesuai UU Terorisme apabila perbuatan itu dilakukan dengan motif ideologi, politik dan gangguan keamanan. Kemudian perbuatan baru bisa dikatakan sebagai tindak pidana terorisme ketika kekerasan atau ancaman kekerasan ditunjukan pada badan dan nyawa seseorang secara langsung, bukan dalam bentuk maupun sarana digital. Lalu serangan cyber-terrorism dengan menyebarkan virus ransomeware yang terjadi dengan motif ekonomi, baru dapat dikualifikasikan sebagai tindak pidana terorisme apabila dapat dibuktikan bahwa uang yang diminta oleh pelaku tersebut digunakan untuk mendanai suatu jaringan organisasi radikal yang memiliki pemahaman yang berbeda mengenai ideologi.

Kemudian untuk menghindari mispresepsi dan sekaligus mempertegas pengaturan hukum pidana terhadap kejahatan cyber-terrorism, bahwa terorisme konvensional merupakan tindakan teror yang dilakukan dengan merusak fasilitas umum dengan senjata sebagai contoh bom dll. Sedangkan terorisme siber ini sesungguhnya pengembangan dari tindak pidana terorisme konvensional karena memiliki modus atau cara yang sama dalam melakukan aksinya sesuai dengan ketentuan Pasal 1 angka 2 UU Terorisme hanya saja dilakukan menggunakan sarana elektronik dan motifnya tidak terbatas hanya pada motif ideologi dan politik saja tetapi sepanjang serangan siber itu ditujukan kepada sistem keamanan negara baik secara langsung maupun melalui fasilitas publik dan objek vital negara lainnya. Hal tersebut mengandung arti bahwa dalam klasifikasi ini juga mencakup tindakan terorisme dengan motif pertentangan ideologi yang dilakukan menggunakan sarana internet.

Penulis sendiri berpendapat, bahwasanya dalam konteks cyber-terrorism tidak diatur dalam berbagai peraturan perundang- undangan. Dalam situasi seperti ini pelaku tindak pidana cyber- terrorism tergolong masih bebas dan leluasa karena belum ada regulasi yang secara pasti dan tegas tertulis expersive verbist dalam instrumen hukum di Indonesia. Tetapi untuk mengantisipasi hal tersebut, penulis berpendapat, untuk mengakomodir kejahatan cyber-terorrorism di Indonesia bisa menggunakan instrumen hukum yang ada yakni pada Pasal 30, Pasal 32, dan Pasal 33 UU ITE dan Pasal 6 UU Terorisme untuk jangka waktu yang sifatnya sementara. Lalu hal tersebut juga harus melihat kasusnya terlebih dahulu, jika memang murni tindak pidana terorisme dilakukan secara konvensional maka menggunakan UU Terorisme dan jika menggunakan sarana internet dalam melakukan tindakan atau aksinya maka menggunakan UU.

4.2. Penerapan Hukum Pidana Yang Dilakukan Kepolisian Dalam Proses Penyidikan Untuk Menangani Kejahatan Cyber-terrorism

Sebagaimana penjelasan mengenai pengaturan hukum pidana terhadap kejahatan cyber-terrorism yang sudah diuraikan sebelumnya, kini perlu diketahui juga bagaimana penerapan hukum pidana terhadap kejahatan cyber-terrorism oleh kepolisian dalam rangka proses penyidikan untuk menangani kejahatan tersebut. Pada tindakan penyelidikan penekanan diletakkan pada perbuatan atau tindakan dalam rangka "mencari dan menemukan" sesuatu peristiwa yang dianggap atau diduga sebagai tindak pidana. Kemudian pada proses penyidikan, titik tekannya terletak pada tindakan "mencari serta mengumpulkan bukti" supaya tindak pidana yang ditemukan dapat menjadi terang, serta agar dapat menemukan dan menentukan pelakunya. Berdasarkan penjelasan tersebut hampir tidak ada perbedaan makna antara keduanya. Antara penyelidikan dan penyidikan adalah dua fase tindakan yang berwujud satu. Lalu keduanya saling berkaitan guna dapat diselesaikan pemeriksaan suatu peristiwa pidana (Yahya Harahap 2018:109).

Proses penyidikan terhadap kejahatan cybercrime terkhusus cyber- terrorism pada dasarnya sama dengan proses penyidikan terhadap proses penyidikan terhadap kejahatan konvensional lainnya. Kemudian yang membedakan adalah dari segi proses penangkapan pelaku kejahatan beserta melakukan koordinasi dengan pihak terkait. Penanganan kejahatan cyber- terrorism tergolong rumit, sebab penyidik harus memastikan keberadaan pelaku, alat yang digunakan dalam melakukan kejahatan tersebut serta menemukan alat bukti dan barang bukti. Terlebih penyidik harus menguraikan dan mengetahui modus operandi pelaku kejahatan cyber- terrorism (Abdul Agis 2017:45).

Kemudian berkaitan dengan tindak pidana cyber-terrorism apakah berbeda dengan illegal access jawabannya adalah berbeda karena konsep illegal access masih dalam tataran kejahatan yang masih sederhana sedangkan cyber-terrorism kejahatan yang membutuhkan penanganan khusus. Namun illegal access adalah bagian dari cyber-terrorism, tidak ada pasal khusus yang mengatur mengenai cyber-terrorism. Berbicara mengenai kejahatan siber, ada lima kata kunci terkait kejahatan siber, antara lain: (Eddy O.S Hiariej 2014:299)

a) Illegal access yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.
b) Illegal interception yakni sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer 70 yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis.
c) Data interference diartikan sebagai sengaja dan tanpa hak melakukan perusakan, penghapusan atau perubahan data komputer.
d) System interference yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap fungsinya sistem komputer.
e) e. Missuse of devices adalah penyalahgunaan perlengkapan computer termasuk program komputer, password komputer, kode masuk.

Berdasarkan uraian di atas kemudian dikaitkan dengan hasil wawancara dengan penyidik dalam rangka upaya penyidik menerapkan hukum pidana terhadap tindak pidana cyber-terrorism. Maka tindak pidana cyber-terrorism mengandung unsur illegal access, data interference, dan system interference. Oleh sebab itu, penulis akan menguraikan terlebih dahulu unsur-unsur yang terdapat dalam tindak pidana cyber-terrorism. Hal tersebut berkaitan juga dengan modus operandinya.

a. Relevansi Modus Operandi Cyber-terrorism dengan UU ITE dan UU Terorisme

Berbicara mengenai illegal access, dalam UU ITE illegal access terdapat dalam Pasal 30 dengan modus operandi Unauthorized Access to Computer System and Service yang merupakan kejahatan yang dilakukan dengan cara menerobos masuk atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah atau tanpa izin dari pemilik sistem jaringan komputer tersebut. Biasanya pelaku kejahatan melakukannya dengan tujuan sabotase (Nur Khalimatus 2012:83).

Kemudian mengenai data interference, dalam UU ITE data interference terdapat dalam Pasal 32 dengan modus operandi cyber sabotage and extortion, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb. Logic bomb merupakan suatu program yang dirancang dan dapat digunakan oleh pelakunya sewaktu-waktu atau tergantung keinginan dari pelaku, dari situ terlihat bahwa informasi yang ada di dalam komputer tersebut dapat terganggu, rusak, bahkan hilang. Hal tersebut menimbulkan sistem jaringan komputer tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.

Terakhir adalah system interference, dalam UU ITE system interference terdapat dalam Pasal 33 dengan modus operandi hampir mirip dengan perbuatan pidana pada data interference. Tindak pidana pada system interference ini adalah perbuatan yang melawan hukum dengan melakukan aktivitas yang mengakibatkan terganggunya sistem elektronik sehingga tidak bisa bekerja sebagaimana mestinya. Berdasarkan uraian tersebut menunjukkan relevansi cyber-terrorism dengan UU ITE sebagai penerapan hukum pidana oleh penyidik kepolisian. Hal tersebut dikarenakan terdapat unsur-unsur perbuatan pidana yang terdapat dalam UU ITE.

Kemudian jika berbicara mengenai modus operandi tindak pidana terorisme konvensional sendiri kaitannya dengan UU Terorisme adalah bahwa terorisme sendiri pada hakikatnya suatu tindak kejahatan ekstrim yang sengaja dilakukan dan direncanakan dengan tujuan menebarkan teror, ancaman, ketakutan serta rasa tidak aman di tengah masyarakat (Wenda Hartarto 2016:381). Lalu modus operandi yang merupakan paradigma klasik dalam tindak pidana terorisme berupa penculikan, penyanderaan, dan menimbulkan kerugian bagi lawan tanpa mengorbankan teroris itu sendiri telah berubah dengan menggunakan paradigma baru berupa pengorbanan teroris atau aksi teror dengan bunuh diri. Selain itu terorisme konvensional kerap dalam melakukan aksinya dengan

memasang rakitan bom. Target sasaran terorisme sendiri biasanya ditempat vital seperti mall, tempat ibadah, hotel dll.

Modus-modus yang digunakan dalam aksinya masih tergolong konvensional. Sehingga menjadi relevan ketika dalam menjerat teroris dengan modus operandi yang dilakukan masih dengan cara konvensional menggunakan instrumen UU Terorisme. Namun dalam perkembangannya, teroris juga memanfaatkan sarana internet dalam menunjang aksinya. Sebagai contoh, pembiayaan aksi terorisme. Pendukung aksi terorisme juga bisa menggunakan sarana internet sebagai lahan pengumpulan dana. Pembiayaan ini pada umumnya dibagi dalam beberapa kategori, yaitu ajakan langsung, e-commerce, eksploitasi alat pembayaran online, dan melakukan pemerasan dengan menyerang komputer yang kemudian meminta uang dalam bentuk bitcoin. Kaitannya dengan cyber- terrorism, yang pada sebelumnya sempat disinggung bahwa Indonesia pernah mengalami serangan cyber-terrorism, kemudian menyerang Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais. Hal itu menyebabkan gangguan komputer sehingga menimbulkan kekacauan. Pelaku membobol jaringan komputer yang kemudian meminta uang dalam bentuk uang virtual. Tetapi kasus tersebut belum diketahui siapa pelakunya.

Berdasarkan keterangan dari Kominfo bahwa kasus serangan itu kategori cyber-terrorism. Berdasarkan hasil wawancara dengan Bapak Iptu Endro Prabowo penyidik Subdit V/Siber Direktorat Reserse Kriminal Khusus Polda Jawa Tengah, bahwa dalam penerapan hukum pidana terhadap tindak pidana cyber-terrorism, beliau mengatakan “terkait dengan cyber-terrorism atau terorisme siber itu perbuatan terornya akan ikut pada UU Terorisme, tapi 74 perbuatan-perbuatan yang mendukung aksinya akan ikut pada UU ITE. Sebagai contoh teroris Imam Samudra, yang dilakukan Imam Samudra melakukan carding. Berdasarkan barang bukti yang ditemukan, Imam Samudra melakukan transaksi untuk menghimpun dana. Kemudian perbuatan Imam Samudra tersebut dalam hal melakukan carding tidak diatur dalam UU Terorisme. Maka perbuatan tersebut, penyidik bisa men-juncto kan kedua UU tersebut”. Menurut hemat penulis, bahwa pengaturan tindak pidana cyber-terrorism belum diatur dalam kedua instrumen hukum tersebut. Tetapi dalam rangka penegakan hukum, khususnya penyidik kepolisian menggunakan instrumen hukum yang ada untuk menerapkan hukum pidana yakni UU Terorisme dan UU ITE sebagai prevensi penyidik dalam penanggulangan tindak pidana cyber-terrorism. Tetapi dalam menerapkan kedua UU tersebut hanya untuk sementara waktu.

b. Proses Penyidik Kepolisian Dalam Mengungkap Tindak Pidana Cyber-terrorism

Dalam proses penyidikan tentu penyidik memiliki mekanisme dalam menangani tindak pidana cyber-terrorism, mengingat tindak pidana cyber-terrorism ini lokasi, pelaku, dan alat yang digunakan tidak berada ditempat yang sama. Berdasarkan hasil wawancara dengan Bapak Iptu Endro Prabowo penyidik Subdit V/Siber Direktorat Reserse Kriminal Khusus Polda Jawa Tengah. Beliau mengatakan “penyidik harus memahami terlebih dahulu mengenai teori locus dan tempus”. Berbicara mengenai tempus delicti, Vos menyatakan bahwasanya

tempus delicti ditentukan pada saat tindakan atau kelakuan terjadi. Berbeda dengan Vos, Jonkers menyatakan bahwa tempus delicti adalah pada saat tindakan atau kelakuan terjadi dan pada saat akibat terjadi. Dasar agrumentasinya perbuatan terdiri dari dua segi yakni tindakan dan akibat (Eddy OS Hiariej 2014:297).

Tindakan dan akibat merupakan suatu rangkaian peristiwa sebagai satu kesatuan yang tidak dapat dipisahkan. Untuk menjerat pelaku penyidik dalam menangani perkara cyber-terrorism menganut pendapat dari Jonkers yakni tempus delicti dapat ditentukan pada saat tindakan akibat terjadi. Kemudian mengenai locus delicti, bapak Iptu Endro Prabowo mengatakan "dalam menentukan locus suatu tindak pidana, penyidik memahami teori locus dalam hukum pidana, ada yang namanya teori perbuatan, kemudian teori bekerjanya alat dan teori akibat". Dalam doktrin hukum pidana ada dua aliran dalam menentukan locus delicti. Pertama, aliran yang menentukan hanya satu tempat terjadinya perbuatan pidana. Kedua, aliran yang menentukan di beberapa tempat terjadinya suatu perbuatan pidana. berdasarkan aliran pertama, ada dua teori, masing-masing adalah teori tentang tempat di mana tindakan terjadi dan teori instrumen. Sedangkan aliran kedua dapat memilih untuk menggunakan teori tempat terjadinya tindak pidana atau memilih menggunakan teori akibat. Khususnya cyber-terrorism, penyidik lebih menggunakan teori instrumen, di mana locus delicti ditentukan oleh alat yang digunakan dan dengan alat itu perbuatan pidana diselesaikan. Penggunaan teori instrumen ini sangat berarti dalam kejahatan-kejahatan yang modus operandinya canggih atau terjadi pada lintas batas.

Dalam kaitanya penanganan tindak pidana cyber-terrorism, bapak Iptu Endro Prabowo menambahkan bahwa "dalam penetuan locus delicti cyber-terrorism khususnya cyber-terrorism ada istilah lain mengenai locus delicti. Istilah dalam siber, yakni teori uploder, teori downloder, dan server. Teori uploder itu sama dengan teori perbuatan di mana perbuatan itu dilakukan. Kemudian teori downloder sama dengan teori akibat sedangkan teori server sama dengan teori bekerjanya alat. Istilah-istilah tersebut hanya diperuntukan untu tindak pidana yang dilakukan menggunakan instrumen jaringan internet.

Kemudian berbicara mengenai proses. Jika penyelidikan ternyata ditemukan paling sedikit 2 (dua) alat bukti sebagaimana yang diatur dalam KUHAP dan/atau khusus yang mengatur mengenai perbuatan yang diduga kejahatan siber, maka penyidik akan melanjutkan proses penyidikan, dengan menerbitkan Surat Dimulainya Penyidikan (SPDP) lalu diberikan kepada Jaksa Penuntut Umum. Selanjutnya dilakukan pemerikasaan, berkaitan dengan proses pemeriksaan barang bukti digital dalam penanganan data elektronik diperlukan langkah khusus agar bukti digital tidak mengalami perubahan. Karena itu penyidik harus memahami penanganan awal barang bukti elektronik pada komputer di tempat kejadian perkara, penggandaan secara physical sektor per sektor (forensic imaging), analisis sistem file (file system), dari program windows, mencari dan memunculkan file walaupun sudah dihapus dan diformat, atau data yang tidak

pernah disimpan dan hanya di print, analisis telepon seluler (mobile forensic), dan analisis gambar digital (image forensic). Selanjutnya pemeriksaan dalam tahap penyidikan dilakukan terhadap saksi, ahli, dan pemeriksaan tersangka. Untuk kepentingan pembuktian tentang persesuaian keterangan saksi dengan saksi, saksi dengan tersangka, tersangka dengan tersangka, dapat dilakukan pemeriksaan konfrontasi dan juga rekonstruksi dan dokumentasi.

Semua pemeriksaan, rekonstruksi dan dokumentasi dibuatkan berita acara. Berkaitan dengan pemerikasaan alat bukti digital dalam proses pemeriksaan pada masa penyidikan diperlukan ahli teknologi informasi yang bersertifikasi, sehingga penyidik dapat melibatkan profesional. Cara kerja ahli digital forensik antara lain:

a) Proses acuqiring dan imaging. Setelah penyidik menerima barang bukti digital, maka harus dilakukan proses acuqiring dan imaging yaitu mengkloning/menduplikat secara tepat dan presisi 1:1. Dari hasil kopi tersebut, seorang ahli digital forensik dapat melakukan analisis.
b) Melakukan analisis. Setelah melakukan proses acuqiring dan imaging, maka dapat dilanjutkan untuk menganalisis isi data terutama yang sudah dihapus, disembunyikan, di-enskrip, dan jejak log file yang ditinggalkan.

Selanjutnya perlu diketahui sasaran pada proses penyidikan khusus cyber-terrorism adalah pelaku, alat yang digunakan, tempat, peristiwa, dan kegiatannya. Menurut hemat penulis, dalam proses penyidikan untuk menangani tindak pidana cyber-terrorism, penyidik dituntut bekerja profesional dalam mengungkap tindak pidana tersebut. Mengingat cyber-terrorism adalah kejahatan yang sangat kompleks dan memiliki tingkat kesulitan yang sangat luar biasa dalam proses penegakan hukum.

5. Kesimpulan

1. Berkaitan dengan pengaturan hukum mengenai tindak pidana cyber- terrorism ini pada hakikatnya belum dirumuskan atau belum diatur dalam sebuah peraturan perundang-undangan. Dalam uraian sebelumnya, penulis melakukan inventarisasi pasal dalam KUHP, UU Telekomunikasi, UU Pendanaan Terorisme, UU ITE, dan UU Terorisme. Berdasarkan hasil kajian dan penelitian, penulis berpendapat instrumen hukum yang paling mendekati dalam mengantisipasi tindak pidana cyber-terrorisme yakni UU ITE dan UU Terorisme. Dasar argumentasinya adalah dalam KUHP sama sekali tidak mengakomodasi tindak pidana cyber-terrorism. Selain itu pasal-pasal dalam KUHP jika dirunut berdasarkan unsurnya maka sudah sangat jelas bahwa rumusan bentuk tindak pidananya masih bersifat konvensional sehingga tidak memenuhi kualifikasi kejahatan cyber- terrorism. Lalu dalam UU Telekomunikasi, UU tersebut hanya diperuntukan untuk mengtur jalannya komunikasi antar penyelenggara. Selanjutnya dalam UU Pendanaan Terorisme jika dikaitkan dengan tindak pidana cyber-terrorism, maka tidak diatur sama sekali mengenai tindak pidana cyber-terrorism. Dalam UU a quo hanya mengatur sebatas transaksinya saja. Kemudian pasal dalam UU ITE, penulis berpendapat bahwa ketentuan Pasal 30, Pasal 32,

dan Pasal 33 memiliki dimensi pengaturan yang dapat mengantisipasi kejahatan cyber-terrorism. Hal tersebut didasari berdasarkan penafsiran unsur-unsur pasal kemudian dikaitkan dengan cara atau modus operandi dari tindak pidana cyber-terrorism. Selanjutnya dalam UU Terorisme, penulis berpendapat setelah menginventarisasi pasal yang termaktub dalam UU Terorisme, maka yang sedikit mendekati adalah Pasal 6 UU Terorisme. itu pun terletak pada frasa ancaman kekerasan yang menimbulkan suasana teror atau rasa takut terhadap orang secara meluas serta menimbulkan korban yang bersifat masal.

2. Dalam proses penyidikan, penyidik memandang perlu pentingnya menguraikan modus operandi cyber-terrorism dengan UU ITE dan Terorisme. Tindak pidana cyber-terrorism mengandung unsur illegal access, data interference, dan system interference. Pada Pasal 30 dengan menggunakan modus operandi Unauthorized Access to Computer System and Service. Kemudian Pasal 32 dengan menggunakan modus operandi cyber sabotage and extortion. Terakhir Pasal 33 dengan menggunakan modus operandi hampir mirip dengan perbuatan pidana pada data interference. Hal ini menurut penulis, modus operandi yang digunakan relevan dengan apa yang ada di dalam UU ITE. Selanjutnya dalam UU Terorisme Modus-modus yang digunakan dalam aksinya masih tergolong konvensional. Sehingga menjadi relevan ketika dalam menjerat teroris dengan modus operandi yang dilakukan masih dengan cara konvensional menggunakan instrumen UU Terorisme.
3. Berdasarkan hasil wawancara yang dilakukan dengan penyidik, terkait dengan cyber-terrorism atau terorisme siber itu perbuatan terornya akan ikut pada UU Terorisme, tapi perbuatan-perbuatan yang mendukung aksinya akan ikut pada UU ITE.

6. Saran

1. Pemerintah dalam hal ini Presiden dan DPR memiliki pilihan dalam membuat kebijakan terkait dengan penanggulangan tindak pidana cyber- terrorism, yaitu merevisi UU ITE atau UU Terorisme dan membuat undang-undang baru dalam rangka untuk mengantisipasi tindak pidana tersebut. Sebab Indonesia saat ini mengalami kekosongan hukum mengenai tindak pidana cyber-terrorism. Kebijakan tersebut bisa dilakukan dengan politik hukum pidana.
2. Aparat penegak hukum dalam hal ini penyidik kepolisian harus meningkatkan profesionalitas dan meningkatkan kemampuan dalam menangani kejahatan siber. Mengingat kejahatan siber ini akan terus berkembang pesat begitu pula dengan modus operandinya.

7. Daftar Pustaka

Buku

Aris Hardinanto. 2019. *Akses Ilegal Dalam Perspekif Hukum Pidana*, Malang: Setara Perss

Barda Nawawi Arief. 2011. Reformasi Sistem Peradilan (Sistem Penegakan Hukum) di Indonesia. Semarang: Universitas Diponegoro

Eddy O.S Hiariej. 2014. *Prinsip-Prinsip Hukum Pidana. Yogyakarta:* Cahaya Atma Pustaka

Moeljatno. 2015. *Asas-Asas Hukum Pidana.* Jakarta: PT Rineka Cipta

Pieter Mahmud Marzuki. 2014. *Penelitian Hukum* (Edisi Revisi). Jakarta: PT. Raja Grafindo Persada

Satjipto Raharjo. 2006. *Membedah Hukum Progresif*, Jakarta: PT Kompas Media Nusantara

Sheila Maulida Fitri. 2020. *Ransomeware Wannacry dan Tindak Pidana Terorisme Siber*, Yogyakarta: Magnum Pustaka Utama

Jurnal

Abdul Agis. 2017. Peranan Kepolisian Dalam Penyidikan Penyalahgunaan Informasi Dan Transaksi Elektronika (ITE). Vol 1 No 2. Makassar: Universitas Muslim Indonesia

Agis Josianto Adam. 2014. Tindak Pidana Cyber Terrorism Dalam Transaksi Elektronik. *Jurnal Lex Administratum*. Vol II No.2.

Ahmad Faizal dan Eko Soponyono. 2020. Kebijakan Hukum Pidana dalam Pengaturan dan Penanggulangan Ujaran Kebencian (Hate Speech) di Media Sosial. Jurnal Pembangunan Hukum Indonesia. Vol 2 No 2. Semarang: Universitas Diponegoro.

Anselmus S. J. Mandagie. 2020. Proses Hukum Tindak Pidana Pembunuhan Yang Dilakukan Oleh Anak Dibawah Umur Ditinjau Dari Undang-Undang Nomor 11 Tahun 2012 tentang Sistem Peradilan Pidana Anak. Lex Crimen Vol. IX/No. 2.

Constantin Georgescu dan Monica Tudor. 2015. Cyber Terrorism Threats to Critical Infrastructures Nato's Role in Cyber Defense. Knowledge Horizons - Economics Journal. Vol 7 No. 2. Romania: Dimitrie Cantemir Christian University Department of Economics and International Affairs

Nur Khalimatus. 2012. Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Transaksi Elektronik. Jurnal Perspektif. Volume XVII No. 2. Surabaya: Universitas Wijaya Kusuma.

Wenda Hartarto. 2016. Analisis Pencegahan Tindakpidana Pendanaan Teroris Pada Era Masyarakat Ekonomi Asean (Analysis of Crime Prevention of Terrorist Financing in Asean Economic Community Era). Jurnal Legislasi Indonesia. Vol. 13 No. 04.

Zephirinus Jondong. 2020. Kebijakan Hukum Pidana Bagi Tindak Pidana Cyber Terrorism Dalam Rangka Pembentukan Hukum Positif Di Indonesia. Jurnal Preferensi Hukum. Vol. 1, No. 2. Bali: Fakultas Ilmu Hukum Universitas Warmadewa

E-ISSN: 2775-2038

Peraturan Perundang-Undangan
Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang.
Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi
Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme Kitab Undang-Undang Hukum Pidana