Jurnal Pembangunan Hukum Indonesia
Volume 3, Nomor 2, Tahun 2021, halaman 228-239

Program Studi Magister Ilmu Hukum
Fakultas Hukum Universitas Diponegoro

Research Article

Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Cyber Terorism

Dwila Annisa Rizki Amalia[1*], Mujiono Hafidh Prasetyo[2]
[1]Program Studi Magister Ilmu Hukum, Fakultas Hukum, Universitas Diponegoro
[2]Fakultas Hukum, Universitas Diponegoro
[*]rizki.amal007@gmail.com

ABSTRACT

In line with the development of community needs in the world, the global community is currently in an era of advancement in science and technology. Not only does this progress have a positive impact, it also has a negative impact. One of the negative impacts of advances in science and technology is the emergence of crimes, one of which is cyber terrorism. The purpose of this article is to find out and analyze criminal law policies in efforts to combat cyber terrorism based on current and future positive law. The research method used is a normative juridical method with literature studies. Based on the results and discussion, the criminal law policy in efforts to combat cyber terrorism based on positive law is currently not explicitly regulated either in the Criminal Code or in special laws outside the Criminal Code. By not regulating the criminal act of cyber terrorism in various applicable laws and regulations, theoretically the perpetrators of cyber terrorism cannot be held accountable because criminal liability takes into account the elements against the law in the formulation of the offense and is related to the principle of legality and elements of error. Meanwhile, the criminal law policy in efforts to tackle cyber terrorism in the future is reviewed through a comparative study and the Draft Criminal Code. The provisions in the comparative study and the Draft Criminal Code can serve as an example in formulating a policy formulation related to specific crimes of cyber terrorism.
Keywords: Penal Policy; Criminal Act; Cyber Terorism.

ABSTRAK

Seiring dengan perkembangan kebutuhan masyarakat di dunia masyarakat global saat ini berada dalam era kemajuan IPTEK. Kemajuan tersebut selain memberikan dampak positif, tetapi juga memberikan dampak negatif. Salah satu dampak negatif dari kemajuan IPTEK adalah timbulnya kejahatan salah satunya adalah cyber terorism. Tujuan dari artikel ini adalah untuk mengetahui dan menganalisis kebijakan hukum pidana dalam upaya penanggulangan tindak pidana cyber terorism berdasarkan hukum positif saat ini dan di masa yang akan datang. Metode penelitian yang digunakan adalah menggunakan metode yuridis normatif dengan studi literatur. Berdasarkan hasil dan pembahasan, Kebijakan hukum pidana dalam upaya penanggulangan tindak pidana cyber terorism berdasarkan hukum positif saat Ini belum diatur secara eksplisit baik dalam KUHP maupun UU khusus di luar KUHP. Dengan tidak diaturnya tindak pidana cyber terrorism dalam berbagai peraturan perundang-undangan yang berlaku, maka secara teoritis pelaku tindak pidana cyber terrorism tidak dapat diminta pertanggungjawabannya karena pertanggungjawaban pidana memperhatikan unsur melawan hukum dalam rumusan delik dan berkaitan dengan asas legalitas serta unsur kesalahan. Sedangkan Kebijakan hukum pidana dalam upaya penanggulangan tindak pidana cyber terorism di masa yang akan datang ditinjau melalui kajian perbandingan dan RUU KUHP. Ketentuan-ketentuan dalam kajian perbandingan dan RUU KUHP tersebut dapat menjadi contoh dalam merumuskan suatu kebijakan formulasi terkait tindak pidana khusus cyber terorism.
Kata Kunci: Kebijakan Hukum Pidana; Tindak Pidana; Cyber Terorism.

A. PENDAHULUAN

Kondisi masyarakat saat ini menjadi lebih terhubung oleh Ilmu Pengetahuan dan Teknologi (IPTEK) daripada sebelumnya dikarenakan sistem telekomunikasi dan komputer dapat terhubung secara global/have global reach. Manfaat kemajuan teknologi informasi dan komunikasi khususnya internet telah menyentuh semua sisi kehidupan manusia modern (Ufran, 2014). Dinamika IPTEK dalam kehidupan masyarakat saat ini selain memberikam dampak positif, tetapi juga memberikan dampak negatif dari ketidaksesuaian penggunaannya (Sudjito dkk, 2016). Ketidaksesuaian penggunaan IPTEK yang mengakibatkan timbulnya suatu kejahatan yang dikenal dengan istilah kejahatan siber (Arief, 2012).

IPTEK telah mengalami evolusi, yang semula digunakan untuk kepentingan militer dan ilmiah menjadi sasaran dan sarana kejahatan. Para pengguna internet tidak saja hanya para ilmuwan, pengguna umum melainkan dipakai oleh mata-mata dan teroris (Jachowicz, 2003). Seiring berjalannya waktu, muncul suatu kejahatan siber yang dikenal dengan istilah cyber terorism.

Cyber terrorism kadang juga disebut dengan cyber sabotage and exortion. Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer atau program komputer tertentu sehingga data, program komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana dikehendaki oleh pelaku.

Untuk itu, diperlukan pemahaman yang memadai mengenai anatomi cyberterrorism. Keutuhan pemahaman mengenai kejahatan yang tergolong baru ini menjadi penting untuk membuat peta jalan yang komperehensif untuk meminimalisir kemampuan teroris untuk melakukan serangan terhadap jaringan ataupun menjadikan komputer sebagai media untuk propaganda teror. Hal ini berkaitan dengan bagaimana kebijakan hukum pidana dalam menanggulangi tindak pidana cyber terorism tersebut.

Kebijakan hukum pidana merupakan kebijakan dari negara melalui badanbadan yang berwenang untuk menerapkan peraturan-peraturan yang dikehendaki yang diperkirakan dapat digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan. Usaha dan kebijakan untuk membuat peraturan hukum pidana yang baik pada hakikatnya tidak dapat dilepaskan dari tujuan penanggulangan kejahatan (Arief, 2014).

Jadi kebijakan atau politik hukum pidana juga merupakan bagian dari politik kriminal. Di lihat dari sudut politik kriminal, maka politik hukum pidana identik dengan pengertian kebijakan penanggulangan kejahatan dengan hukum pidana. Sedangkan menurut Marc Ansel, Kebijakan hukum pidana Kebijakan hukum

pidana merupakan ilmu untuk menyusun atau memformulasikan hukum positif menjadi lebih baik dari yang sebelumnya (Arief, 2014). Berdasarkan hal tersebut, maka perlu dikaji terlebih dahulu bagaimana ketentuan yang saat ini berlaku atau hukum positif yang mengatur mengenai tindak pidana penyebaran pornografi untuk membuat kebijakan yang lebih baik di masa mendatang.

Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya merupakan bagian dari usaha penegakan hukum (khususnya penegakan hukum pidana). Politik hukum pidana merupakan bagian dari kebijakan penegakan hukum (law enforcement policy). Penggunaan upaya hukum termasuk hukum pidana, sebagai salah satu upaya mengatasi masalah sosial termasuk dalam bidang kebijaksanaan penegakan hukum. Disamping itu bertujuan mencapai kesejahteraan masyarakat pada umumnya, maka kebijaksanaan penegakan hukum ini pun termasuk dalam kebijaksanaan sosial, yaitu segala usaha yang rasional untuk mencapai kesejahteraan masyarakat (Arief, 2014).

Kejahatan baru ini sangat berdampak pada dunia usaha. Banyak yang menganggap bahwa keberadaan KUHP tidak mampu menjangkau kejahatan baru tersebut, sehingga pemerintah menginisiasi lahirnya aturan tentang cyber crime. Berdasarkan dokumen yang ada, Undang-Undang Tentang Informasi dan Trsansaksi Elektonik (UU ITE) yaitu Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 (Hermawan, 2019).

Menurut Widodo, penjatuhan pidana penjara para pelaku cyber crime adalah langkah yang kurang bijak. Hal ini disebabkan oleh ketidaksesuaian antara karakteristik pelaku tindak pidana dengan sistem pembinaan narapidana di Lembaga Pemasyarakatan, sehingga tujuan pemidanaan sebagaimana diatur dalam Undan-Undang Pemasyarakatan tidak akan tercapai. Menurut Widodo, sebagai pengganti pemidanaan tersebut adalah pidana kerja sosial atau pidana pengawasan (Widodo, 2013).

Karena ada kesesuaian antara karakteristik pelaku cyber crime dengan paradigma pemidanaan dalam pidana kerja sosial atau pidana pengawasan, sehingga tujuan pemidanaan dapat dicapai.5 Sejalan dengan pandangan Widodo, dalam mengantisipasi cyber crime, Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana (RUU KUHP) mencoba memperluas cakupan istilah untuk dapat membidik dan menjaring kejahatan tersebut.

Sedangkan menurut Barda Nawawi Arief, dalam perspektif hukum pidana, upaya penanggulangan cyber crime dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek pembuktian dan alat bukti), dan aspek yurisdiksi (Djanggih, 2013).

Indonesia mencoba melakukan kebijakan harmonisasi dengan negaranegara lain, khususnya

dalam lingkungan Asia dan Asean menyangkut masalah cyber crime. Antisipasi masalah cyber crime tidak hanya melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), namun juga berusaha mengantisipasinya dalam penyusunan RUU KUHP.

Berdasarkan uraian tersebut, maka permasalahan yang berkaitan dengan kebijakan hukum pidana dalam upaya penanggulangan cyber terorism yang pertama, bagaimana kebijakan hukum pidana dalam upaya penanggulangan tindak pidana cyber terorism berdasarkan hukum positif saat ini? Yang kedua, bagaimana kebijakan hukum pidana dalam upaya penanggulangan tindak pidana cyber terorism di masa yang akan datang?

Beberapa penelitian sebelumnya ada yang membahas mengenai cyber terorism seperti dalam artikel yang ditulis oleh Zephirinus Jondong yang berjudul "Kebijakan Hukum Pidana bagi Tindak Pidana Cyber Terorism dalam Rangka Pembentukan Hukum Positif di Indonesia" (Jondong, 2020). Selain itu, penelitian lainnya menguak aksi cyber teorirsm era media beru seperti yang ditulis oleh Eska Nia Sarinastiti dan Nabilla Kusuma Vardhani (Sarinastiti, & Vardhani, 2018). Berkaitan dengan artikel tersebut, ada sebuah penelitian yang ditulis oleh Lee Jarvis dkk yang berjudul "Constructing Cyberteorism As A Security Threat: A Study of International News Media Coverage" (Jarvis, Macdonald, & Whiting, 2017). Selanjutnya mengarah pada penyebab timbulnya suatu cyber prostitution, ada sebuah penelitian yang ditulis oleh Zahri Yunos dan Sharifuddin Sulaman dengan judul "Understanding Cyber Terorism From Motivational Perspective" (Yunos, & Sulaman, 2017). Terakhir, ada suatu artikel penelitian yang membahas mengenai upaya penanggulangan cyber terorism seperti yang ditulis oleh Rizky Reza Lubis yang berjudul "Potensi Pengguna Internet Indonesia dalam Counter-Cyber Radicalization" (Lubis, 2017).

Artikel-artikel tersebut tidak membahas mengenai upaya penanggulangan cyber terorism melalui kebijakan hukum pidana untuk merumuskan suatu ketentuan atau hukum yang lebih baik di masa mendatang. Dalam artikel ini tentunya akan membahas hal tersebut dengan kajian ius constitutum dan ius constituendumnya. Artikel ini tentunya menggunakan bahan kajian terbaru seperti RUU KUHP 2019 yang tidak pernah dibahas dalam penelitian-penelitian sebelumnya, ditambah dengan adanya kajian komparasi dengan negara-negara lain untuk menjawab permasalahan yang ada.

B. METODE PENELITIAN

Metode penelitian yang digunakan adalah menggunakan metode yuridis normatif dengan studi literatur. Studi literatur meneliti data sekunder berupa bahan hukum primer dan bahan hukum sekunder. Dalam penelitian ini menganalisis Peraturan Perundang-Undangan yang berkaitan dengan tindak pidana penyebaran pornografi, yaitu KUHP, UU Telekomuniksi dan UU ITE serta RUU KUHP yang di

masa mendatang akan menjadi Peraturan Perundang-Undangan di Indonesia. Selain itu, dalam penelitian ini juga melakukan kajian perbandingan dengan negara-negara lain terkait dengan pengaturan tindak pidana cyber terorism.

Metode yang digunakan untuk menganalisis data yang terkumpul dalam penelitian ini adalah metode analisis kualitatif. Penelitian yuridis normatif yang bersifat kualitatif adalah penelitian yang mengacu pada norma hukum yang terdapat dalam peraturan perundang-undangan dan putusan pengadilan serta norma-norma yang hidup dan berkembang dalam masyarakat (Soekanto, & Mamudji, 2004).

C. HASIL DAN PEMBAHASAN

1. Kebijakan Hukum Pidana dalam Upaya Penanggulangan Tindak Pidana Cyber Terorism berdasarkan Hukum Positif Saat Ini

a. Kitab Undang-Undang Hukum Pidana (KUHP)

Kitab Undang-Undang Hukum Pidana yang disingkat KUHP merupakan sistem induk bagi peraturan-peraturan hukum pidana di Indonesia. Meskipun KUHP ini merupakan buatan penjajah Belanda namun untuk saat ini karena belum ada perubahan atau penerimaan atas pembaharuan KUHP yang telah dilakukan oleh para ahli hukum pidana Indonesia yang telah diupayakan sejak tahun 1963 maka KUHP yang ada ini harus tetap dipergunakan demi menjaga keberadaan hukum pidana itu sendiri dalam masyarakat Indonesia.

Perumusan tindak pidana di dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan cyber terorism yang merupakan bagian dari cyber crime. Di samping itu, mengandung berbagai kelemahan dan keterbatasan dalam mengahadapi perkembangan teknologi dan high tech crime yang sangat bervariasi.

Berkaitan dengan hal itu, apakah KUHP dapat digunakan dalam menanggulangi tindak pidana CT yang merupakan bagian dari cyber crime, berikut identifikasinya: 1). Kejahatan terhadap ketertiban umum Bab V Pasal 168 ayat 1,2,dan 3; 2). Kejahatan terhadap nyawa Bab XIX Pasal 340; 3). Pencurian Bab XXII Pasal 362; 4). Pemerasan dan pengancaman Bab XXIII Pasal 368.

Berkaitan dengan permasalahan tersebut, jika KUHP ingin digunakan untuk menanggulangi tindak pidana cyber terorism haruslah diperhatikan terlebih dahulu batasan-batasan atau ruang lingkup dan unsur-unsur/bentuk-bentuk cyber terorism yang telah penulis uraikan, sehingga dapat dikatakan sebagai tindak pidana cyber terorism.

Unsur-unsur tersebut antara lain: Serangannya melalui dunia maya bermotivasi politik yang dapat mengarah pada kematian luka-luka; Menyebabkan ketakutan atau merugikan secara fisik atas tekhik serangan dari dunia maya tersebut; Serangannya serius untuk melawan atau ditujukan ke infrastruktur informasi kritis seperti keuangan, energi, transportasi

dan operasi pemerintah; Serangan yang mengganggu sarana yang tidak penting, bukan dikategorikan sebagai aksi cyber terrorism; dan Serangan itu tidaklah semata-mata dipusatkan pada keuntungan moneter.

b. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Kualifikasi delik yang diatur dalam Undang-Undang Telekomunikasi mengenai cyber terorism diatur dalam Pasal 47-59 yang dikualifikasikan sebagai kejahatan. Berdasarkan ketentuan pidana dari Pasal 47 sampai dengan Pasal 59, beberapa Pasal di antaranya dapat diidentifikasi unsur tindak pidananya sebagai berikut: Pasal 47 dengan unsur tindak pidana: penyelenggaraan jaringan telekomunikasi yang tanpa izin dari menteri; Pasal 50 dengan unsur tindak pidana: melakukan perbuatan tanpa hak, tidak sah atau memanipulasi, akses ke jaringan telekomunikasi dan/atau akses kejasa telekomunikasi dan/atau akses ke jaringan ke telekomunikasi khusus; Pasal 52 dengan unsur tindak pidana: memperdagangkan, membuat, merakit, memasukan dan/atau menggunakan perangkat komunikasi di wilayah Indonesia tanpa memenuhi syarat tekhnis dan ijin; Pasal 53 dengan unsur tindak pidana: pengunaan spektrum frekwensi radio dan orbit satelit tanpa ijin pemerintah dan tidak sesuai dengan peruntukannya dan saling menganggu; Pasal 55 dengan unsur tindak pidana: melakukan perbuatan yang menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi; Pasal 56 dengan unsur tindak pidana: melakukan penyadapan informasi yang disalurkan melalui jaringan telekomunikasi; dan Pasal 57 dengan unsur tindak pidana: tidak menjaga kerahasiaan infomasi yang dikirim dan/atau diterima oleh pelanggan.

Mengenai unsur sifat melawan hukum, dalam Undang-Undang Telekomunikasi tersebut tidak disebutkan secara tegas, namun demikian unsur ‘sifat melawan hukum’ tersebut dapat dilihat pada perumusan seperti dirumuskan dalam Pasal 47 sampai dengan Pasal 57, sehingga dapat disimpulkan bahwa dengan tidak disebutkannya secara tegas unsur sifat melawan hukum terlihat ada kesamaan ide dasar antara UU Telekomunikasi dengan Konsep KUHP baru yang sekarang tengah disusun yang menentukan bahwa meskipun unsur sifat melawan hukum tidak dicantumkan secara tegas, tetapi suatu delik harus tetap dianggap bertentangan dengan hukum.

Disamping itu walaupun kata “dengan sengaja” tidak dicantumkan secara tegas, namun jika dilihat dari unsur-unsur tindak pidana yang ada, maka tindak pidana yang dilakukan didasarkan pada unsur kesengajaan (dolus). Jika dilihat dari unsur-unsur perbuatan yang dilarang seperti disebutkan di atas maka dapat diidentifikasikan perbuatan yang dilarang (unsur tindak pidana) yang erat kaitannya dengan penyalahgunaan internet untuk tujuan cyber terorism yaitu sebagaimana disebutkan dalam Pasal 22 berupa Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: a). akses ke jaringan

telekomunikasi; dan atau, b). akses kejasa telekomunikasi; dan atau, c). akses ke jaringan telekomunikasi khusus, (Terkait dengan aksi kejahatan CT yang berbentuk Unathorized acces to computer system and service); Pasal 38 berupa Setiap orang dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi, (Terkait dengan aksi kejahatan Cyber sabotaje and extortion); Pasal 50 berupa melakukan perbuatan tanpa hak, tidak sah atau memanipulasi, akses ke jaringan telekomunikasi dan/atau akses ke jasa telekomunikasi dan/atau akses ke jaringan ke telekomunikasi khusus', (Terkait dengan aksi kejahatan Unathorized acces to computer system and service); dan Pasal 52 berupa memperdagangkan, membuat, merakit, memasukan dan/atau menggunakan perangkat komunikasi di wilayah Indonesia tanpa memenuhi syarat tekhnis dan ijin (Terkait dengan aksi kejahatan Carding).

Berdasarkan ketentuan yang telah dikriminalisasikan dalam Undang-undang Telekomunikasi tersebut, nampak adanya kriminalisasi terhadap perbuatan-perbuatan yang berhubungan dengan penyalahgunaan penggunaan internet, yang berbentuk tindak pidana cyber terorism.

c. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Berdasarkan ketentuan pasal-pasal dalam Bab XI mengenai ketentuan pidana dalam UU ITE, maka dapat diidentifikasikan beberapa perbuatan yang dilarang (unsur tindak pidana) yang erat kaitannya dengan tindak pidana cyber terorism pada tiap-tiap pasalnya sebagai berikut: Pasal 30 dengan unsur tindak pidana : megakses, menerobos, menjebol Sistem Komputer atau Sistem Elektronik milik orang lain secara illegal. (Terkait dengan aksi kejahatan cyber terorism yang berbentuk unauthorized acces to computer system dan service); Pasal 31 dengan unsur tindak pidana: melakukan intersepsi/ penyadapan secara illegal atas Informasi Elektronik dan/atau Sistem Ellektronik dalam suatu komputer dan/atau Sistem Elektronik tertentu milik orang lain. (terkait dengan aksi kejahtan Hacking); Pasal 32 dengan unsur tindak pidana: melakukan transmisi merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik. (Terkait dengan aksi kejahatan cyber terorism yang berbentuk cyber sabotage dan extortion); Pasal 33 dengan unsur tindak pidana : melakukan tindakan apa pun secara illegal yang berakibat terganggunya Sistem Elektronik menjadi tak bisa bekerja. (Terkait dengan aksi kejahatan cyber terorism yang berbentuk unauthorized acces to computer system dan service) (Vadza, 2013); Pasal 34 dengan unsur tindak pidana : memperoduksi, menjual mengadakan untuk digunakan, mengimpor, menyediakan perangkat lunak komputer untuk tujuan kesusilaan atau eksploitasi seksual terhadap anak, penyadapan, merusak, dan menghilangkan suatu Informasi Elektronik dan/atau

Dokumen Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik. (Terkait dengan aksi kejahatan CT yang berbentuk Hackng, Cyber saborage dan extortion); Pasal 35 dengan unsur tindak pidana : melakukan perubahan, penciptaan, perusakan, penghilangan dan memanipulasi data Informasi Elektronik/ Dokumen Elektronik dengan tujuan Informasi dan/ atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik (Terkait dengan aksi kejahatan Hacking).

Mengenai unsur sifat melawan hukum, dalam UU ITE tersebut disebutkan secara tegas, unsur 'sifat melawan hukum tersebut dapat dilihat pada perumusan Pasal 30 sampai dengan Pasal 37 tersebut di atas, sehingga dapat disimpulkan bahwa dengan disebutkannya secara tegas unsur sifat melawan hukum terlihat ada kesamaan ide dasar antara UU ITE dengan KUHP yang masih menyebutkan unsur sifat melawan hukumnya suatu perbuatan. Berbeda dengan Konsep KUHP baru yang sekarang tengah disusun yang menentukan bahwa meskipun unsur sifat melawan hukum tidak dicantumkan secara tegas, tetapi suatu delik harus tetap dianggap bertentangan dengan hukum.

Melihat berbagai ketentuan yang telah dikriminalisasikan dalam Undang-undang ITE tersebut, nampak adanya kriminalisasi terhadap perbuatan-perbuatan yang berhubungan dengan penyalahgunaan penggunaan di bidang teknologi Infomasi dan Transaksi Elektronik, yang berbentuk tindak pidana cyber terorism (Natsir, 2009).

2. Kebijakan Hukum Pidana dalam Upaya Penanggulangan Tindak Pidana Cyber Terorism di Masa yang Akan Datang

a. Kajian Perbandingan dengan Negara Lain

(1) Singapura

Di Singapura pengaturan mengenai penyalahgunaan internet/computer crime yang mengarah kepada tindak pidana cyber terorisn di atur khusus di dalam UU di luar KUHP nya. Beberapa ketentuan dalam perundang-undangan Negara Singapura berkaitan dengan perbuatan cyber terorism yaitu dalam Chapter 50A;Computer missue Act Unauthorized access to computer material Section 3 sebagai berikut:

(1) "Any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offense and shall be liable on conviction to a imprisonment for a term not exceeding 2 years or to both and, in case of a second or subsequent for a term not exceeding 3 years or to both. (1) If any damage is caused as a restut of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50.000 or to imprisonment for a term not exceeding 7 years or to both. Section 4: Accesswith intent to commit or facilitate commission of offence. (1) Any person who causes a computer

to perform any function for the purpose of securing access to any computer with intent to commit this section applies, shall be guilt of an offence."

(2) "This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years."

(3) "Any person guilty of an offence under this section shall be liable on conviction to a not exceeding $50.000 or to imprisonment for a term not exceeding 10 years pr to both."

Berdasarkan ketentuan tersebeut di atas, dapat disimpulkan bahwa setiap orang yang mengakses komputer yang tanpa hak/secara illegal yang dapat mengarah kepada perbuatan cyber terorism dipidana penjara paling sedikit 2 (dua) sampai dengnan 3 (tiga) tahun, kemudian apabila menyebabkan program dan data komputer terganggu di pidana penjara selama 7 (tujuh) sampai dengan 10 tahun penjara dan denda $50.000.

Dalam sudut pandang kebijakan hukum pidana, hal tersebut terjadi sebuah kriminalisasi terhadap suatu perbuatan tertentu dan adanya perluasan delik yang mengarah kepada tindak pidana cyber terorism.

(2). Belgia

Di Belgia pengaturan mengenai penyalahgunaan internet (cyber crime) diatur dalam penal code atau KUHP. Ketentuan-ketentuan yang berkaitan dengan cyber crime yang merujuk pada aksi kejahatan cyber terorism ditambahkan pasal baru dalam KUHP Belgia yang berlaku efektif pada tahun 2001.

Bentuk cyber terorism yang diatur yaitu mengenai aksi kejahatan Hacking seperti yang termuat dalam Article 550 (b) of the Criminal Code :

Section 1. "Any person who, aware that he is not authorized, accesses or maintains his acces to computer system, may be sentencedto a term of imprisonment of 3 months to 1 years and to a fine of (Bfr 5,200-5m) or to one of these sentences. If the offences specified in section 1 above is committed with intention of defraud, the term of imprisonment may be from 6 months to years."

Section 2. "Any person who, with the intention to defraud or with the intention to cause harm, exceeds his power of access to a computer system, may be sentenced to term of imprisonment of 6 months to 2 years and to a fine of (BFr 5, 200-20m) or to one of these sentences."

Section 3. "Any person finding himself in one of the situations specified in saction 1 and 2 who either: accesses data which is stored, processed or transmitted by a computer system, or procures such data in any way whatsoever, or makes any use whatsoever, or couse any damage, even unintentionally, to a computer system, or data which is stored, processed or transmitted by such a system may be sentenced to term of imprisonment of 1 to 3 year and to a fine of (BFr 5, 200-10m) or to one of these sentenced."

Pasal tersebut menegaskan setiap orang yang tanpa hak atau secara illegal mengakses sistem informasi diancam pidana 3 (tiga) tahun penjara dan denda 5 (lima) milyar, jika melakukan penipuan terhadap sistem informasi tersebut dipidana penjara 3 (tiga) bulan hingga 1 (satu) tahun, jika menyebabkan kerusakan terhadap data dalam komputer atau sistem informasi di ancam pidana penjara 1 (satu) sampai dengan 3 (tiga) tahun dan denda 10 (sepuluh) milyar.

Sama halnya dengan negara Singapura, ketentuan di negara Belgia terdapat suatu perumusan yang lebih eksplisit terkait dengan tindak pidana cyber terorism yang dapat dikenakan terhadap pelaku tindak pidana cyber terorism tersebut.

b. RUU KUHP 2019

Ketentuan yang berkaitan dengan tindak pidana terhadap Informatika dan Telematika kaitannya dengan cyber terorism di dalam RUU KUHP 2019 diatur dalam Pasal 336 sampai dengan Pasal 339. Berikut identifikasi unsur-unsur tindak pidananya.

Pasal 336 dengan unsur tindak pidana : mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer dan/atau sistem elektronik; (terkait dengan aksi kejahatan cyber terorism yang berbentuk Unauthorized acces computer system and sevice, Hacking, dan Cyber sabatoge dan extortion).

Pasal 337 dengan unsur tindak pidana : mengakses komputer, dan/atau sistem elektronik tanpa hak, yang menyebabkan gangguan atau bahaya terhadap negara dan/atau hubungan dengan subjek hukum internasional; (Terkait dengan aksi kejahatan Unauthorized acces computer system and service).

Pasal 338 dengan unsur tindak pidana : mengakses komputer dan/atau sistem elektronik tanpa hak memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi; (terkait dengan aksi kejahatan cyber terorism yang berbentuk Unauthorized acces computer system and sevice, Hacking, dan Cyber sabatoge dan extortion).

Pasal 339 dengan unsur tindak pidana : mengakses komputer dan/atau sistem elektronik tanpa hak dengan maksud memperoleh keuntungan atau memperoleh informasi keuangan dari Bank Sentral, lembaga perbankan atau lembaga keuangan, penerbit kartu kredit, atau kartu pembayaran atau yang mengandung data laporan nasabahnya; (terkait dengan aksi kejahatan cyber terorism yang berbentuk Unauthorized acces computer system and sevice, dan Carding). Jika dicermati isi pasal-pasal tersebut, secara jelas dan terinci adanya kriminalisasi terhadap perbuatan cyber terorism, Pasal-Pasal tersebut mengarah kepada kriminalisasi terhadap tindak pidana cyber terorism.

D. SIMPULAN

Kebijakan hukum pidana dalam upaya penanggulangan tindak pidana cyber terorism berdasarkan hukum positif saat Ini belum diatur secara eksplisit baik dalam KUHP maupun UU khusus di luar KUHP. Dengan tidak diaturnya tindak pidana cyber terrorism dalam berbagai peraturan perundang-undangan yang berlaku, maka secara teoritis pelaku tindak pidana cyber terrorism tidak dapat diminta pertanggungjawabannya karena pertanggungjawaban pidana memperhatikan unsur melawan hukum dalam rumusan delik dan berkaitan dengan asas legalitas serta unsur kesalahan. Dalam mewujudkan penegakan hukum perlu peran aktif aparat penegak hukum yaitu dengan dibekali keahlian khusus dalam melakukan penyidikan dan penyelidikan guna memperlancar pembuktian kejahatan mayantara (cyber crime) khususnya terhadap tindak pidana cyber terorism tersebut.

Kebijakan hukum pidana dalam upaya penanggulangan tindak pidana cyber terorism di masa yang akan datang ditinjau melalui kajian perbandingan dan RUU KUHP. Ketentuan-ketentuan dalam kajian perbandingan dan RUU KUHP tersebut dapat menjadi contoh dalam merumuskan suatu kebijakan formulasi terkait tindak pidana khusus cyber terorism. Sehubungan dengan hal tersdebut dan untuk mewujudkan penal reform, maka seyogyanya perlu secepatnya mengesahkan/melegitimasi RUU KUHP 2019 agar sistem induk dalam hukum pidana tersebut dapat sesuai dengan perkembangan masyarakat Indonesia saat ini.

DAFTAR PUSTAKA

JURNAL

Djanggih, H. (2013). Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan. Jurnal Media Hukum, Vol.1, (No.2), p.3.

Hermawan, R. (2019). Kesiapan aparatur pemerintah dalam menghadapi cyber crime di Indonesia. Jurnal Media Hukum, Vol.6, (No.1), pp.3-4.

Jarvis, Lee., Macdonald, Stuart., & Whiting, Andrew. (2017). Constructing Cyberteorism As A Security Threat: A Study of International News Media Coverage. Europan Journal of International Security, Vol.2, (Issue1), pp.64-87.

Jondong, Z. (2020). Kebijakan Hukum Pidana bagi Tindak Pidana Cyber Terorism dalam Rangka Pembentukan Hukum Positif di Indonesia. Jurnal Preferensi Hukum, Vol.1, (No.2), pp.21-27.

Lubis, Rini R. (2017). Potensi Pengguna Internet Indonesia dalam Counter-Cyber Radicalization. Jurnal Pertahanan dan Bela Negara, Vol.7, (No.2), pp.19-34.

Sarinastiti, Eska Nia., & Vardhani, Nabilla Kusuma. (2018). Internet dan Terorisme: Menguatnya Aksi Global Cyber-Terorism Melalui New Media. Jurnal Gema Societa, Vol.1, (No.1), pp.40-52.

Sudjito, Bambang., Majid, Abdul., Sulistio, Faizin., & Ruslijanto, Patricia Audrey. (2016). Tindak Pidana Pornografi dalam Era Siber di Indonesia. Jurnal Wacana, Vol.19, (No.2), p. 1.

Ufran. (2014). Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyber Terorism. Masalah-Masalah Hukum, Vol.43, (No.4), p.1.

Vadza, K. (2013). Cybercrime and its Categories. Indian Journal of Applied Research, Vol.3, (Issue.5), pp.180.

Yunos, Zahri., & Sulaman, Sharifuddin. (2017). Understanding Cyber Terorism From Motivational Perspective. Journal of Information Warfare, Vol.16, (Issue4), pp.41-59.

ARTIKEL DALAM PROSIDING

Jachowicz, L. (2003). Cyberterrorism And Cyberhooliganism: How To Prevent And Fight International and Domestic, In Proceedings at Collegium Civitas Foreign Policy of the United States of America (p.4), New York.

TESIS

Natsir, Nanda I. (2009). Kebijakan Kriminal terhadap Tindak Pidana Cyber Terorism. Universitas Diponegoro

BUKU

Arief, Barda N. (2014). Bunga Rampai Kebijakan Hukum Pidana (Perkembangan Penyusunan Konsep KUHP Baru). Jakarta: Kencana.

Arief, Barda N. (2012). Kapita Selekta Hukum Pidana. Bandung: Citra Aditya Bhakti.

Soekanto, Soerjono., & Mamudji, Sri. (2004). Penelitian Hukum Normatif Suatu Tinjaua Singkat. Jakarta: Grafindo Persada.

Widodo. (2013). Sistem Pemidanaan dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime. Yogyakarta: Laksbang Mediatama.