JURISDICTIE	P-ISSN 1693-5918	Naskah dikirim: 05/08/2021	Naskah direview: 13/10/2021	Naskah diterbitkan: 20/12/2021
Hlm 35-63				

PENANGGULANGAN TINDAK PIDANA *CYBER TERRORISM* DALAM PERSPEKTIF KEPASTIAN HUKUM

Arvid Gema Indrawan [1] Abdul Haris Semendawai [2] Wiryanto [3]

[1] *Anggota Perhimpunan Advokat Indonesia, Indonesia, arvidgema@gmail.com*

[2] *Universitas Islam As-Syafi'iyah, Indonesia, ahsemendawai@hmail.com*

[3] *Universitas Islam As-Syafi'iyah, Indonesia, wiryanto@gmail.com*

ABSTRACT

One example of the Cyber terrorism case committed by Bahrumsyah and M. Bahrun Naim, who is known to have transferred funds to make car bombs to ISIS support groups in Solo. So based on the crimes committed by Bahrun in getting money from the ISIS group in Syria, while the money sent to his network in Indonesia was carded. The main problem of this research is law enforcement in the prevention of cyber terrorism according to Indonesian positive law, and the legal provisions for tackling cyber terrorism from the perspective of legal certainty. This research is included in the normative juridical research typology with secondary data types, so as to produce research in the form of prescriptive analytical through literature studies. The results of this study reveal that there is no law enforcement in the prevention of cyber terrorism. 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 offenses and is related to the principle of legality and elements of guilt. The lack of certainty in tackling cyber terrorism is due to the higher frequency of technology use with a developing system, with the existing convergance of media. It is hoped that it can provide legal certainty that comprehensively regulates the movement and use as well as irregularities in cyber crime that uses computers as the main tool and benefits of the developing technological media

Keywords: Prevention, Crime, Cyber Terrorism, Legal Certainty

PENDAHULUAN

Cyber terrorism merupakan salah satu jenis *cyber crime* dari beberapa jenis-jenis *cyber crime* yang ada, yang muncul akibat dari dampak negatif perkembangan sarana teknologi informasi dan komunikasi masyarakat global, sehingga terjadi perubahan-perubahan pola perilaku masyarakat dalam bidang ini sebagai penyalahgunaan komputer. Tujuannya melumpuhkan infrastruktur secara nasional, seperti energi, transportasi, untuk menekan/ mengintimidasi kegiatan-kegiatan pemerintah atau masyarakat sipil.

Cyber terrorism dapat disebut juga dengan istilah *cyber sabotage and exortion*. Karena kejahatan ini bertujuan untuk membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung ke internet. Modus operandi kejahatan *Cyber terrorism* dilakukan dengan menyusupkan suatu virus komputer atau program komputer tertentu sehingga data, program komputer tidak dapat digunakan, atau berjalan sebagaimana dikehendaki oleh pelaku.[1]

Untuk itu, diperlukan pemahaman yang memadai mengenai anatomi *cyber terrorism*. 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. Informasi yang didapat secara cepat, tepat dan akurat memainkan peranan sangat penting dalam berbagai aspek kehidupan manusia, seperti penentuan sebuah kebijaksanaan, sebagai alat bantu dalam proses pengambilan keputusan atau bahkan sebagai tren atau gaya hidup manusia modern. Kenyataannya semakin banyak kalangan bisnis, organisasi, perkantoran, pendidikan dan militer hingga individu yang menjadi sangat ketergantungan dengan fenomena zaman informasi ini. Sehingga munculah istilah yang sering dikenal dengan sebutan "*the information age*" atau abad informasi.[2]

Namun kemudahan serta kenikmatan yang ditawarkan pada abad informasi saat ini sekaligus mengundang para terorisme di dunia maya *(cyber terrorism*) untuk turut serta didalamnya. Pengertian tentang *cyber terrorism* itu sendiri sebenarnya terdiri dari dua aspek yaitu *cyber space* dan *terrorism*, sementara para pelakunya disebut dengan *cyber terrorists*. Para *hackers* dan *crackers* juga dapat disebut sebagai *cyber terrorist*, karena seringkali kegiatan yang dilakukan mereka di dunia maya dapat menteror serta menimbulkan dampak kerugian yang besar terhadap korban yang menjadi targetnya, mirip seperti layaknya aksi terorisme. Keduanya mengeksploitasi dunia maya untuk kepentingannya masing-masing. Adapun perbedaan antara *cyber terrorist* dan *hackers* yang terletak pada motivasi dan tujuannya, dimana para *cyber terrorist* bermotivasi untuk kepentingan politik kelompok tertentu dengan tujuan memperlihatkan eksistensinya dipanggung politik dunia. Sementara para *hackers* mempunyai motivasi untuk memperlihatkan eksistensinya atau adu kecakapan untuk menunjukan superioritasnya di dunia maya dengan tujuan kepuasan tersendiri atau demi uang.

Teroris memerupakan kejahatan terhadap kemanusiaan dan peradaban serta merupakan salah satu ancaman serius terhadap kedaulatan setiap negara. Karena, teroris memerupakan kejahatan yang bersifat internasional yang menimbulkan bahaya terhadap keamanan, perdamaian dunia, serta merugikan kesejahteraan masyarakat. Maka, perlu dilakukan penanggulangan secara berencana dan berkesinambungan, sehingga hak asasi orang banyak dapat dilindungi dan dijunjung tinggi.

Terorisme salah satu kejahatan kemanusiaan yang tergolong ke dalam *Extra Ordinary Crime* (Kejahatan luar biasa), semua orang sepakat bahwa aksi terorisme yang mengorbankan bahkan membunuh warga sipil tak berdosa tidak bisa dibenarkan. Sehingga terorisme adalah kejahatan yang berlabel *Extra Ordinary Crime* dan harus ditangani dengan *Extra Ordinary Measure* (penanganan tindakan luar biasa).[3]

Pernyataan tersebut sejalan dengan tujuan bangsa Indonesia yang termaktub dalam UUD 1945 yaitu melindungi segenap bangsa Indonesia, dan seluruh tumpah darah Indonesia, dan untuk memajukan kesejahteraan

[1] H. Sutaman, *Cyber Crime, Modus Operandi dan Penangulangannya*, (Jogjakarta: LeksBang Pressindo, 2007), hal. 83.

[2] James A. Lewis, *Op. Cit*.

[3] Muhammad Ikhlas Thamri, *Densus 88 Undercover*, (Solo: Quo Vadis, 2007), hal. 74.

umum, mencerdaskan kehidupan bangsa dan ikut melaksanakan ketertiban dunia. Indonesia sebagai negara hukum memiliki kewajiban untuk melindungi harkat dan martabat manusia. Demikian pula dalam hal perlindungan warga negara dari tindakan terorisme. Salah satu bentuk perlindungan negara terhadap warganya dari tindakan aksi terorisme adalah melalui penegakan hukum termasuk didalamnya menciptakan produk hukum yang sesuai.

Upaya ini diwujudkan pemerintah dengan membuat peraturan yaitu tentang Tindak Pidana menggunakan sarana internet di Indonesia diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang diundangkan pada tanggal 21 April Tahun 2008 dan telah mengalami perubahan pada tanggal 25 November 2016 dengan terbitnya Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Sedangkan Tindak Pidana Penanggulangan Terorisme sendiri juga telah diatur dalam 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, yang diundangkan pada tanggal 4 April 2003 dan telah mengalami perubahan pada tanggal 22 Juni 2018 dengan terbitnya 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.

Oleh karena dampak dari aksi terorisme yang dirasakan langsung oleh masyarakat. Petaka yang ditimbulkan tidak hanya korban jiwa yang banyak, kerugian yang besar, namun juga menimbulkan berdampak yang luas pada banyak hal terkait kehidupan berbangsa dan bernegara.[4] Tak dapat dipungkiri lagi teroris telah merasuk ke dalam lini kehidupan masyarakat. Seperti virus, terorisme telah menyebar selama puluhan tahun ke berbagai kalangan di Tanah Air. Jika sebelumnya, penyebarannya memanfaatkan lembaga pendidikan dan tempat ibadah, kini kehadiran internet semakin memudahkan penularan virus radikalisme.[5]

The Jakarta Post (2019) mencatat bahwa pengguna internet di Indonesia telah mencapai hingga 64,8% dari total populasi (sekitar 171 juta pengguna) pada tahun 2018 dan masih terus berkembang. Kemudahan menggunakan media *online* sebagai alat komunikasi juga memudahkan kelompok teroris untuk berinteraksi, perkembangan kelompok-kelompok teroris di Indonesia tidak hanya melalui studi, rekrutmen kader dan pelatihan militer, tetapi juga melalui propaganda. Suatu perbuatan pidana yang dilakukan para pelaku menggunakan dunia *cyber terrorism* untuk menyebarkan provokasi. Isi propaganda sebagian besar kritik terhadap kinerja pemerintah atau kegiatan lain yang tidak sejalan dengan tujuan teroris. Selain itu, propaganda mereka bukan pandangan netral dan lebih diarahkan untuk mendiskreditkan pemerintah dan bahkan mendesak publik untuk mendukung aksi teror.

Adapun jenis pelanggaran *Cyber terrorism* seperti:

1. Pengendalian dan pengelolaan jaringan terorisme melalui internet ke seluruh dunia, penggalangan dana dengan cara carding.
2. Komunikasi antar teroris via internet dengan pembangunan strategi melalui situs web khusus dan atau aplikasi media sosial sebagai media untuk mengoordinasikan semua kegiatan dalam pelaksanaan aksi teror.
3. Melakukan pencucian uang dari hasil pembobolan kartu kredit di sejumlah situs perjudian.[6]

Cyber terrorism telah banyak terjadi, baik di negara Indonesia maupun negara-negara lainnya. Dari data yang diperoleh mengenai kejahatan *cyber terrorism* tersebut diantaranya, beberapa waktu lalu di tahun 2016, Uang miliaran rupiah dari Suriah masuk Indonesia. Berdasarkan penelusuran Detasemen Khusus 88 Kepolisian RI (Densus 88 Anti Teror), uang

[4] Agus Surya Bakti, *Deradikalisasi Nusantara, Perang Semesta Berbasis Kearifan Lokal MelawanRadikalisasi dan Terorisme*, (Jakarta: Daulat Press, 2016).
[5] *Ibid*.
[6] Eska Nia Sarinastiti1 dan Nabilla Kusuma Vardhani, *Internet dan Terorisme: Menguatnya Aksi Global Cyber Terrorism Melalui New Media*, Januari 2018.

itu bermuara pada Bahrumsyah dan Bahrun Naim. Uang tersebut diduga digunakan *Islamic State of Iraq and Syria* (ISIS) Indonesia untuk aksi teror.

Muhammad Bahrun Naim Anggih Tamtomo telah ditetapkan polisi sebagai tersangka otak di balik teror bom di Jalan M.H. Thamrin, Jakarta, Kamis, 14 Januari 2016. Data Densus 88 AT, Bahrun mengirim uang Rp 40-70 juta, tidak lama sebelum pengeboman terjadi. Pengiriman dilakukan secara bertahap. Bahrun Naim tidak hanya dikaitkan dengan bom Jalan M.H. Thamrin. Berdasarkan temuan *Institute for Policy Analysis of Conflict* (IPAC), Bahrun diketahui pernah mentransfer dana untuk membuat bom mobil kepada kelompok pendukung ISIS di Solo, Jawa Tengah, di bawah pimpinan Ibad Durrahman dan Arif Hidayatullah. Jadi berdasarkan tindak kejahatan yang dilakukan oleh Bahrun dalam mendapatkan uang dari kelompok ISIS di Suriah, sementara uang yang dikirim kepada jaringannya di Indonesia merupakan hasil *carding*.[7]

Dalam mempromosikan situs-situ web dan forum diskusi *online* tersebut kelompok teroris cenderung menggunakan jaringan sosial media. Selain itu, sosial media dipahami sebagai instrumen yang cukup relevan dan efektif dalam *cyber radicalization*. Salah satu contohnya adalah kasus perekrutan 25 calon "jihadis" melalui media sosial *Facebook* untuk dikirim ke Suriah pada tahun 2014, diantaranya adalah WNI yang telah dideportasi dari Turki dan diperiksa sebagai saksi. Menurut keterangannya, mereka akan berangkat ke Suriah dengan mendapatkan akses dari pertemanan di *Facebook*. Awal mulanya, saksi tersebut mendapat undangan pertemanan di *Facebook* dengan seseorang yang tidak dikenal, saksi menerima pertemanan tersebut karena melihat tulisan-tulisan di halaman *Facebook* yang sangat Islami dan banyak bercerita mengenai daulah atau daerah kekuasan ISIS di Suriah. Pertemanan di *Facebook* tersebut berlanjut dengan memanfaatkan fasilitas chat secara personal yang pada akhirnya mendapatkan tawaran untuk berangkat ke Suriah.[8]

Contoh tersebut di atas menunjukkan salah satu bentuk dalam mempromosikan ideologi radikal dan menggalang dukungan melalui sosial media. Sosial media yang paling sering digunakan adalah sosial media yang paling banyak peminatnya, dimana tiga teratas adalah *Facebook*, *Youtube* dan *Twitter*.[9] Perkembangan *Islamic State of Iraq and Syria* (*ISIS*) dari gerakan lokal di Irak menjadi gerakan transnasional hingga menyebar ke Indonesia. Apa yang disebut sebagai Negara Islam (*ISIS*) setelah ekspansi fenomenalnya di tanah air telah menjadi sangat aktif dan inovatif di bidang *cyber* teror. Sejumlah organisasi dan individu telah menyatakan kesetiaan kepada *ISIS* dan menggunakan taktik siber mereka sejalan dengan strategi siber organisasi teroris ini.[10]

Sebagaimana telah dibincangkan di muka, bahwa terorisme selalu menggunakan kekerasan dalam memaksakan kehendaknya dan menimbulkan kerusakan, kehancuran, bahkan kematian orang banyak yang tidak berdosa. Pola dan cara-cara seperti itu jelas bertentangan dengan ajaran Islam, karena Islam diturunkan sebagai rahmatan lil'alamin, bukan untuk menimbulkan kerusakan, ketakutan, kehancuran dan perselisihan, Islam berarti kedamaian. Ajaran Islam mengedepankan sikap inklusif, toleran, tasamuh, menghargai setiap perbedaan. Sangat banyak ayat Al-Qur'an yang melarang kekerasan, pembunuhan dan perusakan di muka bumi. Allah SWT menyamakan orang yang membunuh dan melakukan perusakan di muka bumi sama dengan membunuh seluruh manusia, sebagaimana difirmankan dalam surat Al-Maidah ayat 32.

Dari ayat tersebut jelas bahwa terorisme yang terkadang memakan korban jiwa manusia yang tidak bersalah dan menimbulkan kerusakan adalah bertentangan dengan ajaran Islam.Sebagaimana diketahui bahwa menurut pengertian bahasa, jihad berasal dari kata juhd (Bahasa Arab) yang berarti kemampuan, atau mengeluarkan sepenuh tenaga dan kemampuan

[7] Wahyono, Edi dalam investigasi, merekrut dibalik jeruji, news, 2016.
[8] Petrus Reinhard Golose, *Op. Cit*.
[9] Rizky Reza Lubis Alumni Universitas Pertahanan Indonesia, Potensi Pengguna Internet Indonesia Dalam Counter-Cyber Radicalization Indonesia's Netizen Potential On Counter-Cyber Radicalization.
[10] Eksistensi dan Perkembangan *ISIS*: Dari Irak Hingga Indonesia, Najamuddin Khairur Rijal Prodi Hubungan Internasional, Universitas Muhammadiyah Malang.

dalam mengerjakan sesuatu. Kata jihad juga berasal dari kata Jahd (Bahasa Arab) yang berarti kesukaran yang untuk mengatasinya harus dilakukan dengan sungguh-sungguh. Jihad juga berarti perang. Singkatnya, menurut pengertian bahasa, jihad berarti bekerja keras, bersungguh-sungguh, mengerahkan seluruh kemampuan untuk menyelesaikan suatu masalah atau mencapai tujuan yang mulia. Pengertian lain jihad adalah mengerahkan segala kemampuan untuk menangkis serangan dan menghadapi musuh yang tidak tampak yaitu hawa nafsu setan dan musuh yang tampak yaitu orang kafir yang memusuhi Islam. Jihad dalam pengertian ini tidak hanya mencangkup pengertian perang melawa musuh yang memerangi Islam tetapi lebih luas lagi, jihad berarti berusaha sekuat tenaga dan kemampuan untuk mengalahkan nafsu setan dalam diri manusia.[11]

Taufik Makaro, menjelaskan dalam jurnal hukumnya tentang Pemberantasan Terorisme di Indonesia adalah merupakan salah satu masalah yang sangat penting dan menarik untuk dikaji dan diteliti karena berkaitan dengan perwujudan tujuan bangsa Indonesia yaitu melindungi seluruh bangsa Indonesia, meningkatkan kesejahteraan masyarakat, mencerdaskan kehidupan bangsa dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial. Selain itu juga terorisme telah menghabiskan nyawa tanpa melihat korban dan menimbulkan ketakutan masyarakat secara luas, atau hilangnya kebebasan, serta kerugian harta benda. Selanjutnya karena terorisme mempunyai jaringan yang luas sehingga merupakan ancaman terhadap perdamaian dan keamanan nasional maupun internasional.[12]

Untuk itu, diperlukan pemahaman yang memadai mengenai anatomi *cyber terrorism*. 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. Insiden *cyber* merupakan kejadian yang mengganggu berjalannya sistem elektronik misalnya serangan virus, pencurian data, informasi pribadi, hak kekayaan intelektual perusahaan dan gangguan akses terhadap layanan informasi elektronik. Mekanisme *work from home* semakin memperbesar potensi risiko karena pekerjaan harus dilakukan melalui jaringan. Pandemi Covid-19 harus disikapi oleh organisasi sebagai momentum untuk membenahi kebijakan keamanan informasi untuk mengantisipasi insiden siber. Persiapan yang baik akan memperkecil kerugian akibat pencurian informasi atau gangguan pada layanan dan insiden siber berkembang menjadi lebih luas. Pemulihan sistem dan data elektronik yang terdampak insiden perlu dilakukan sesegera mungkin sehingga organisasi dapat melanjutkan proses bisnis dan kegiatannya. Informasi yang diperoleh selama penanganan insiden dapat digunakan sebagai dasar langkah perbaikan dan persiapan penanganan insiden dikemudian hari. Jika memang diperlukan, bukti kejadian serangan *cyber* bisa digunakan untuk mendukung langkah hukum.

Beberapa rumusan delik dalam 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 dan UU ITE dapat digunakan bagi pelaku *cyber terrorism*. Namun hal ini dinilai belum mampu untuk menjerat pelaku tindak pidana teroris didunia mayakarena cakupan dan muatan pengaturan dalam dunia maya yang begitu luas. Saat ini *cyber terrorism* telah menjadi isu besar di setiap Negara.[13]

Oleh karena itu, perlu dilakukan dengan segera sebuah tindakan antisipasi berupa pembaharuan hukum pidana atau kebijakan hokum pidana oleh pembuat undang-undang. Politik hukum menurut Sudarto adalah kebijakan dari negara melalui badan yang berwenang untuk menciptakan ketentuan-ketentuan yang dikehendaki sesuai dengan apa yang sedang berkembang dalam masyarakat dan untuk mencapai apa yang dicita-citakan[14]

Kebijakan hukum pidana dalam tujuannya untuk menegakkan hukum dan menanggulangi tindak pidana *cyber terrorism*

[11] Yusuf Qardhawi, *Fiqih Jihad: Sebuah Karya Monumental Terlengkap Tentang Jihad Menurut Al-Qur'an dan Sunnah*, (Bandung: Mizan, Cet. I, 2010), hal. 1.

[12] *Ibid*., hal. 2.

[13] Sarinastiti & Vardhani, 2018; Ufran, 2014.

[14] Sudarto, *Hukum dan Hukum Pidana*, (Bandung: Alumni, 1981), hal. 159.

pada tulisan ini terbatas pada aspek perumusan tindak pidana dari segi materiil berupa bagaimana perumusan suatu delik. Berdasarkan kondisi sebagaimana diuraikan dalam latar belakang masalah tersebut, ada kekosongan norma terkait penegakan hukum *cyber terrorism*, yakni tidak diaturnya pengaturan mengenai terorisme dunia maya dalam Undang-Undang Nomor 9 Tahun 2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme serta Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Perpu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-undang (yang selanjutnya disingkat menjadi UU Terorisme). Oleh karena itu, penelitian ini berupaya untuk menjelaskan keterkaitan dengan seperangkat isu-isu yang berkaitan dengan *cyber terrorism*. Selain itu juga kedepan perlu dipikirkan tentang kebijakan hokum pidana dalam mengeleminir terjadinya *cyber terrorism* sebagai *trend of crime* ke depan.[15]

Terkait dengan hal-hal sebagaimana diuraikan dalam latar belakang tersebut di atas, penelitian ini hanya terbatas pada ruang lingkup yang berkaitan dengan *cyber terrorism* di Indonesia dengan perumusan masalah mengenai bagaimana penegakan hukum dalam penanggulangan tindak pidana *cyber terrorism* menurut hukum positif Indonesia? dan bagaimana ketentuan hukum penanggulangan tindak pidana *cyber terrorism* dari perspektif kepastian hukum?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian normatif yang bersifat deskriptif analitis yang merupakan penelitian untukmenggambarkan dan menganalisa masalah yang ada dan termasuk dalam jenis penelitian kepustakaan (*library research*) yang akan disajikan secara deskriptif. Pendekatan yang dilakukan pendekatan yuridis, pendekatan normatif dan pendekatan sosiologis. Jenis dan Sumber Data. Dalam metode riset data primer dan sekunder. Teknik pengumpulan data menggunakan wawancara (*interview*) dan instrumen angket/kuesioner dan *online*. Teknik analisis data dilakukan secara sistematis, kualitatif, komprehensif dan lengkap.

PEMBAHASAN DAN ANALISIS

A. Penanggulangan Tindak Pidana *Cyber Terrorism*

Cyber terrorism merupakan salah satu bagian dari tindak pidana *cyber crime* atau perbuatan yang menyalahgunakan teknologi internet yang dapat mengakibatkan kepanikan/ketakukan, kerugian secara fisik dan psikis terhadap individu maupun masyarakat dan menyerang sarana infrastrukstur penting suatu negara, sehingga mengakibatkan kerugian besar bagi targetnya. Jika dilhat dari sudut metode pendekatan teknologi (*techno prevention*)[16] ini, untuk menahan gencarnya penyalahgunaan pemakain internet oleh para kaum hacker dan cracker/CT, Beberapa langkah yang dapat dilakukan dalam pengamanan sistem informasi berbasis interenet antara lain:[17] Mengatur akses (*access control*), Menutup *service* yang tidak digunakan, Memasang proteksi, Firewall, Pemantau adanya serangan, Pemantau integritas sistem, Audit: mengamati berkas log, dan Back up secara rutin.

1. Penggunaan enkripsi untuk meningkatkan keamanan

   Etika penggunaan internet ini dikenal dengan nama *cyber ethics*, yang berisi:[18]

   > Setiap orang harus bertanggungjawab terhadap perilaku sosial dan hukum tatkala menggunakan internet; Tidak seharusnya ikut serta dalam berbagai bentuk saiber yang mengganggu;Seharusnya tidak bercakap-cakap tentang satu apapun kepada orang lain yang tidak dikenal di internet; Mengcopy atau men-*download* program yang berhak cipta, *games* atau musik tanpa ijin atau tanpa membayar adalah perbuatan illegal; Untuk menghindari plagiat/*plagiatism* penting

[15] Ufran, *dalam journal tentang Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism,* Fakultas Hukum Universitas Mataram, Oktober 2014.

[16] Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana*, (Jakarta: Raja Grafindo Persada, 2002), hal. 254-255.

[17] Budi Rahadjo, Op. Cit, hal. 51.

[18] *http//www.ParentNews Safety.com, cyber ethics: Everyone should practice responsible social and legal behavior while on the Internet. No one should participate in any form of cyber-bullying*.

untuk memberi kredit terhadap situs yang digunakan untuk riset; Tidak ada penggemar pada komputer pribadi yang berkirim surat satu sama lain atau saling membacanya; Jangan pernah bermaksud menyebarkan virus komputer; Internet tidak bersifat pribadi dan apa yang anda lakukan atau katakan akan kembali kepada anda.

Maka hal-hal dapat diupayakan guna menanggulangi tindak pidana *cyber terrorism***,** yaitu:

a. Pengenalan komputer dan internet kepada masyarakat. Upaya ini dapat ditempuh dengan jalan sebagai berikut :[19]
   1) Pengenalan Komputer dan Internet Lewat Pendidikan

      Penandatanganan nota kesepakatan antara PT Indosat dan Departemen Pendidikan Nasional (Depdiknas) tentang pengembangan *Cyber Education (CE),* di Malang Jawa Timur, merupakan salah satu upaya pengenalan komputer dan internet kepada masyarakat sejak usia dini. Prinsip dasar *Cyber Education* cukup sederhana, yakni memamfaatkan teknologi *multimedia* internet untuk menyalurkan suatu materi dari satu tempat ke tempat lain. Untuk itu, tempat-tempat yang bersangkutan harus terhubung dalam jaringan komunikasi berbasis protokol internet. PT Indosat, melalui anak perusahaannya Indosat Multi Media, menyediakan infrastruktur sekaligus menyiapkan koneksi internet yang menghubungkan antar lokasi dalam satu jaringan. Depdiknas secara bertahap mengembangkan jaringan internet ke sekolah-sekolah di Kabupaten/Kota seluruhIndonesia. Pada tahap awal, jaringan sekolah dibentuk ditujuh kota sebagai proyek percontohan, yaitu Jakarta, Bandung, Surabaya, Malang, Yogjakarta, Solo dan Makasar. Di setiap kota disiapkan suatu jaringan yang disebut *Wide Area Network* (WAN) kota untuk menghubungkan sekolah satu dengan yang lainnya. Dengan dibangunnya jaringan antar sekolah tersebut maka data pendukung, referensi, ataupun berbagai informasi lain yang relevan dapat diperoleh dengan cepat dan mudah. Selain itu, juga dapat dilakukan diskusi dan pengajaran jarak jauh.
   2) Seminar Teknologi Informasi

      Seminar teknologi informasi sangat membantu pengenalan teknologi computer dan internet kepada mayarakat dalam bentuk diskusi interaktif, bedah buku teknologi informasi, seminar dan lokakarya, *workshop* dan sebagainya. Untuk memperkaya wawasan peserta, juga didatangkan para ahli dari institusi yang terkait erat dengan dunia internet, yaitu APNIC, IndoCISC, Polri, Kejaksaan, Kelompok Pengguna Linux Indonesia (KPLI), dan sebagainya.

b. Peran Serta Masyarakat dalam bidang komputer dan internet

   Sistem keamanan bukan hanya tanggungjawab polisi semata, namun juga menjadi tanggung jawab bersama seluruh elemen masyarakat. Dalam pandangan konsep ini masyarakat dapat sebagai subjek maupun objek. Maksud subyek, masyarakat adalah pelaku aktivitas komunikasi antara yang satu dengan yang lain, serta pengguna jasa kegiatan internet dan media lainnya. Dan obyek, masyarakat dijadikan sasaran dan korban kejahatan bagi segenap aktivitas kriminalisasi internet. Tanggung jawab bersama atas keamanan dan ketertiban di tengah masyarakat dalam konsep modern disebut *Community Policing.* Salah satu model pengamanan dan penegakan hukum yang professional di negara-negara maju. Semua elemen masyarakat dengan kesadaran penuh terpanggil dan bertanggung jawab atas keamanan dan ketertiban. Dilibatkannya masyarakat dalam strategi pencegahan kejahatan mempunyai dua tujuan pokok,

[19] Sutarman, *Cyber Crime, Modes Operandi dan Penanggulangannya*, (Jogjakarta: LaksBang Pressindo, 2007), hal. 101-102.

Upaya penanggulangan (penal) tindak pidana *cyber terrrorism* dalam hukum positif Di Indonesia

Cyber space dapat dikatakan sebagai dunia para teroris untuk melaksanakan aksinya seperti pengeboman. Para teroris menggunakan media teknologi informasi untuk saling berkomunikasi, berkoordinasi, dan melaksanakan agenda mereka. Meskipun terorisme dilakukan melalui dunia maya dengan memanfaatkan teknologi informasi, namun tetap pada dasarnya memiliki motivasi politik dan sosial atas serangan-serangan yang hendak dilakukan terhadap infrastruktur-infrastruktur yang dimiliki oleh negara, seperti keuangan, energi, transportasi, dan operasi pemerintah, sehingga mengakibatkan kematian terhadap orang, rasa takut dalam masyarakat, kelumpuhan ekonomi dalam suatu negara, maupun kelumpuhan infrastruktur negara tersebut.

Berdasarkan uraian tersebut, maka secara umum *cyber terrorism* adalah suatu bentuk tindakan melawan hukum yang direncanakan oleh seseorang atau kelompok orang dengan motivasi politis untuk mencapai ideologinya, baik secara langsung maupun tidak langsung, dengan cara melakukan serangan, penyusupan, mencuri, ataupun merusak data informasi, sistem komputer, program komputer, sehingga dapat menimbulkan korban.

Cyber terrorism memiliki 2 (dua) bentuk karakteristik, yakni *cyber terrorism* sebagai tindakan teror terhadap sistem komputer, jaringan, dan atau basis dan informasi yang tersimpan dalam komputer, serta *cyber terrorism* sebagai penggunaan internet oleh para teroris untuk keperluan organisasi dan media teror kepada pemerintah dan masyarakat. Indonesia memiliki pengaturan di bidang *cyber law* dan pengaturan di bidang terorisme.

Meskipun *cyber terrorism* merupakan bagian dari bentuk kejahatan *cyber crime* sebagaimana yang telah diuraikan sebelumnya, namun satu hal yang harus dipahami bahwa sesuai dengan pendapat Denning,[20] *cyber terrorism* merupakan konvergensi dari *cyber space* dan terorisme. Oleh karena itu, unsur terorisme dalam *cyber terrorism* juga harus diperhatikan karena kejahatan terorisme memiliki motif tersendiri.

Aksi teorisme merupakan tindakan seorang atau kelompok orang yang ingin mempertahankan hidup individu dan kolektif kelompoknya, dengan upaya yang dilakukan secara keliru yaitu mengancam dan membahayakan kelangsungan hidup orang lain. Itu berarti tindak pidana kejahatan teroris harus dilarang dan pelakunya dihukum dalam ketentuan hukum.

Terkait pengaturan khusus *cyber terrorism* belum ada, walaupun Indonesia telah memiliki beberapa ketentuan Undang-undang yang terkait dengan *cyber terrorism*. Sejauh mana sebenarnya kebutuhan akan *cyber law* sebagai *lex specialis* pada pengaturan *cyber terrorism.* Perlu dimasukan secara khusus pengaturan tindak pidana *cyber terrorism* pada ketentuan Hukum Dunia maya (*cyber law*) yang sejatinya kebutuhannya telah mendesak untuk digunakan. Ini disebabkan semakin tinggi frekuensi penggunaan teknologi dengan sistem yang berkembang, dengan konvergensi media (*convergance of media*) yang ada.

Pengaturan mengenai *cyber terrorism* dalam *cyber law* diharapkan bisa memberikan kepastian tegas dalam penjelasan hukum mengenai pengaturan kejahatan *cyber terrorism* secara khusus. Tentunya memiliki alasan utama yaitu adanya aspek yang terkait dengan kejahatan tindak pidana *cyber terrorism* yang dipertegas secara komprehensif dalam sebuah ketentuan undang-undang *cyber law* yang mengatur pergerakan dan penggunaan serta penyimpangan dalam tindakan kejahatan *cyber* yang menggunakan komputer sebagai alat utama dan kemanfaatan dari media teknologi yang berkembang. Artinya tidak hanya bergantung pada satu Undang-Undang (*umbrella act*) saja, meski kita tahu telah ada Undang-Undang Nomor 5 Tahun 2003, ataupun Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, atau Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Memang secara yuridis dalam penyelesaian masalah hukum tindak pidana *cyber terrorism* ini hakim yang menangani harus melakukan penemuan hukum melalui penafsiran dan konstruksi hukum. Namun demikian bila pembangunan hukum nasional mengapresiasi hadirnya *cyber law* secara terintegrasi akan menjadi sebuah penguatan kepastian hukum yang lebih baik, mengingat

[20] *Ibid.*

banyak sekali gerakan terkait tindak pidana terorisme semakin berkemang dengan pola komunikasi dalam kemanfaatan media yang ada, sebagai alat komunikasi untuk melakukan aksi kejahatannya.

Kebijakan formulasi hukum pidana yang berkaitan dengan masalah tindak pidana *cyber terrorism* di bidang *cyber crime* dapat diidentifikasikan sebagai berikut:

1. Kitab Undang-Undang Hukum Pidana Indonesia (KUHP)

   Untuk menghadapi masalah pemalsuan kartu kredit dan transfer dana elektronik saja, KUHP mengalami kesulitan karena tidak ada ketentuan khusus mengenai perbuatan kartu kredit palsu. Ketentuan yang ada hanya mengenai:

   a. Sumpah/keterangan palsu, Bab IX Pasal 242;
   b. Pemalsuan mata uang dan uang kertas Bab X Pasal 244-252;
   c. Pemalsuan materai dan merek, Bab XI Pasal 253-262;
   d. Pemalsuan surat, Bab XII Pasal 263-276.[21]

   Berkaitan dengan hal itu, apakah KUHP dapat digunakan dalam menanggulangi tindak pidana *Cyber terrorism* yang merupakan bagian dari *cyber crime,* berikut identifikasi penulis:

   a. Kejahatan terhadap ketertiban umum Bab V Pasal 168 ayat 1,2,dan 3;
   b. Kejahatan terhadap nyawa Bab XIX Pasal 340;
   c. Pencurian Bab XXII Pasal 362;
   d. Pemerasan dan pengancaman Bab XXIII Pasal 368.

   Berkaitan dengan permasalahan tersebut, jika KUHP ingin digunakan untuk menanggulangi tindak pidana *cyber terrorism* haruslah diperhatikan dulu batasan-batasan, unsur- unsur dan bentuk-bentuk *cyber terrorism* yang telah penulis uraikan, sehingga dapat dikatakan sebagai tindak pidana *cyber terrorism.* Jadi dari penjelasan di atas mengenai unsur-unsur dan bentuk- bentuk tindak pidana *cyber terrorism,* maka penulis berkesimpulan bahwa KItab Undang-Undang Hukum Pidana, tidak dapat digunakan dalam menanggulangi tindak pidana *cyber terrorism.*

2. Undang-Undang Nomor 11 Tahun 2008 Jo. Undang-Undang Nomor 19 Tahun 2016 tentang tentang Informasi Dan Transaksi Elektronik

   Dalam Kongres PBB X tersebut dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan ketentuan yang berhubungan dengan kriminalisasi, pembuktian dan prosedur (*States shouldseek harmonization of relevan provision on criminalization, evidence, and procedure*)[22] dan negara-negara Uni Eropa yang telah secara serius mengintegrasikan regulasi yang terkait dengan pemanfaatan teknologi informasi ke dalam instrumen hukum positif (*existing law*) nasionalnya. Undang-Undang Informasi dan Transaksi Elektronik merupakan undang-undang, Sistem Perumusan Pertanggungjawaban pidana dalam Undang-Undang ITE

   Melihat perumusan ketentuan pidana dalam Undang-Undang ITE sebagai mana diatur dalam Pasal 45 sampai dengan Pasal 52 maka dapat diidentifikasikan bahwa pelaku tindak pidana atau yang dapat dimintakan pertanggunjawaban pidana dalam Undang-Undang ITE adalah meliputi individu atau orang per orang dan korporasi. Ini terbukti dari ketentuan pasal-pasal tersebut yang diawali dengan kata “Setiap orang ” dan “Korporasi”.

   Masalah pertanggungjawaban pidana berkaitan erat dengan pelaku tindak pidana. Pelaku yang dapat dipidana adalah orang dan korporasi, yang dijelaskan dalam Pasal 1 sub 21 dan dalam ketentuan pidana UU ITE tersebut. UU ITE mengatur secara lanjut dan terperinci tentang ketentuan pertanggungjawaban pidana terhadap korporasi, karena UU ITE tersebut membedakan pertanggung jawaban pidana terhadap individu dan korporasi, sebagaimana yang tercantum dalam Pasal 52 UU ITE.

   a. Sistem perumusan sanksi pidana, jenis-jenis sanksi dan lamanya pidana dalam UU ITE

[21] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*, (Jakarta: Raja Grafindo Persada, 2006).

[22] *Ibid*, hal. 5.

Sistem perumusan sanksi pidana dalam Undang-undang ITE adalah alternatif kumulatif. Hal ini bisa dilihat dalam perumusannya yang menggunakan *kata "dan/atau". Jenis*-jenis saksi *(strafsoort)* pidana dalam Undang-undang ITE ini ada dua jenis yaitu pidana penjara dan denda. Sistem Perumusan lamanya pidana (*strafmaat*) dalam Undang-Undang ITE ini adalah:

1) Maksimum khusus, pidana penjara dalam UU ITE paling lama 12 tahun.
2) Maximum khusus pidana dendanya, paling sedikit sebanyak Rp 300.000.000,00 (tiga ratus juta rupiah), dan paling banyak Rp 12.000.000.000,00 (dua belas milyar rupiah).

Berdasarkan pembahasan di atas maka dapat diketahui bahwa Undang-Undang Nomor 11 tahun 2008 tentang Informasi, dan Transaksi Elektronik Jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ("UU ITE") dapat digunakan untuk menanggulangi jenis tindak pidana *cyber terrorism,* sebagai suatu fenomena/bentuk baru *cyber crime* secara umum. Undang-undang ini menekankan pada pengaturan keamanan penggunaan Sistem Informasi Eleketronik atau Dokumen Elektronik, dan mengarah pada penyalahgunaan Informasi Eleketronik untuk tujuan perbuatan-perbuatan *cyber terrorism*.

3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Telekomunikasi terdiri dari kata "tele" yang berarti jarak jauh (*at a distance*) dan "komunikasi" yang berarti hubungan pertukaran ataupun penyampaian informasi, yang didefinisikan oleh Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi sebagai setiap pemancaran, pengiriman informasi melalui medium apapun. Undang-undang ini diundangkan pada tanggal 8 September 1999 dalam Lembaran Negara RI tahun 1999 Nomor 154, dengan Peraturan pelaksananya yaitu PP Nomor 52 tahun 2000 tentang Peraturan Pemerintah tentang Penyelenggaraan Telekomunikasi Indonesia dalam Lembaran Negara nomor 107 tahun 2000, TLN 3980.

Salah satu pertimbangan dalam penyusunan Undang-undang telekomunikasi adalah bahwa pengaruh globalisasi dan perkembangan teknologi komunikasi yang sangat pesat telah mengakibatkan perubahan yang mendasar dalam penyelenggaraan dan cara pandang terhadap telekomunikasi. Penulis mencoba untuk mengkaji masalah *cyber terrorism* ini dengan Undang-undang Telekomunikasi dengan pertimbangan bahwa jaringan internet merupakan salah satu alat atau sarana telekomunikasi yang dapat digunakan untuk memasukan dan menerima informasi, sehingga orang dapat saling melakukan komunikasi/hubungan walaupun berada di tempat yang berjauhan.

a. Sistem perumusan tindak pidana dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Ketentuan pidana dalam Undang-Undang Nomor 36 tahun 1999 tentang Telekomunikasi terdapat dalam Bab VII Pasal 47 sampai dengan Pasal 57, berikut beberapa perumusan pasal dalam ketentuan pidananya :

Pasal 47, menyatakan barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

Pasal 48, penyelenggara jaringan telekomunikasi yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 19 dipidana dengan pidana penjara paling lama 1 (satu) tahun dan / atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).

Pasal 52, barang siapa memperdagangkan, membuat, merakit, memasukkan, atau menggunakan perangkat

telekomunikasi di wilayah Negara Republik Indonesia yang tidak sesuai dengan persyaratan teknis sebagaimana dimaksud dalam Pasal 32 ayat (1), dipidana dengan pidana penjara paling lama 1 (satu) tahun dan atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).

Pasal 59, perbuatan sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51, Pasal 52, Pasal 53, Pasal 54, Pasal 55, Pasal 56, dan Pasal 57 adalah kejahatan. Kualifikasi delik yang diatur dalam Undang-undang Telekomunikasi tersebut diatur dalam Pasal 59 yang dikualifikasikan sebagai kejahatan. Berdasarkan ketentuan pidana dari Pasal 47 sampai dengan Pasal 59 di atas, beberapa Pasal di antaranya dapat diidentifikasi unsur tindak pidananya sebagai berikut:

1) Pasal 47 dengan unsur tindak pidana: penyelenggaraan jaringan telekomunikasi yang tanpa izin dari menteri;
2) 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;
3) Pasal 52 dengan unsur tindak pidana: memperdagangkan, membuat, merakit, memasukan dan/atau menggunakan perangkat komunikasi di wilayah Indonesia tanpa memenuhi syarat tekhnis dan ijin;
4) Pasal 53 dengan unsur tindak pidana: pengunaan spektrum frekwensi radio dan orbit satelit tanpa ijin pemerintah dan tidak sesuai dengan peruntukannya dan saling menganggu;
5) Pasal 55 dengan unsur tindak pidana: melakukan perbuatan yang menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi;
6) Pasal 56 dengan unsur tindak pidana: melakukan penyadapan informasi yang disalurkan melalui jaringan telekomunikasi; dan
7) 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 "melanggar ketentuan sebagaimana dimaksud Pasal 47 sampai dengan Pasal 57 tersebut di atas, sehingga dapat disimpulkan bahwa dengan tidak disebutkannya secara tegas unsur "sifat melawan hukum" terlihat ada kesamaan ide dasar antara Undang-Undang Nomor 36 Tahun 1999 tentang 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 dilihatdari 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 terrorism* yaitu sebagaimana disebutkan dalam:

1) Pasal 22 berupa "Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi: akses ke jaringan telekomunikasi; dan atau, akses kejasa telekomunikasi; dan atau, akses ke jaringan telekomunikasi

khusus", (Terkait dengan aksi kejahatan *Cyber Terorism* yang berbentuk *Unathorized acces to computer system and service*).

2) 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*).
3) 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
4) 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*).

Melihat berbagai 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 *Cyberterrorism.* Jika dicermati lebih lanjut, dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi tersebut ada pasal yang sebenarnya jika terjadi suatu pelanggaran dapat dikenai pidana tetapi hal tersebut justru tidak diatur secara lebih lanjut, yaitu pada Bagian Kelima tentang Hak dan Kewajiban Penyelenggara dan Masyarakat, yang dapat dilihat dalam perumusannya sebagai berikut:

Pasal 21: Penyelenggara telekomunikasi dilarang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, keamanan, atau ketertiban umum.

Terhadap pelanggaran Pasal 21 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi tersebut di atas, hanya dikenakan sanksi administratif saja sebagaimana disebutkan dalam Pasal 45 dan 46 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi:

Pasal 45: Barang siapa melanggar ketentuan Pasal 16 ayat (1), Pasal 18 ayat (2), Pasal 19, Pasal 21, Pasal 25 ayat (2), Pasal 26 ayat (1), Pasal 29 ayat (1), Pasal 29 ayat (2), Pasal 33 ayat (1), Pasal 33 ayat (2), Pasal 34 ayat (1), atau Pasal 34 ayat (2) dikenai sanksi administrasi.

Pasal 46: Sanksi administrasi sebagaimana dimaksud dalam Pasal 45 berupa pencabutan izin. Pencabutan izin sebagaimana dimaksud pada ayat (1) dilakukan setelah diberi peringatan tertulis.

Jika terjadi pelanggaran terhadap Pasal 21 tersebut di atas nampak tidak ada sanksi pidananya dan hanya sebatas sanksi administratif saja**,** yang juga tidak diatur dalam pasal-pasal yang lain. Padahal baik terhadap kepentingan umum, kesusilaan, keamanan dan ketertiban umum sebagaimana disebut dalam Pasal 21, kesemuanya memiliki kepentingan hukum yang juga harus senantiasa dilindungi dengan melalui hukumpidana. Kaitannya dengan hal-hal yang bertentangan dengan kekepentingan umum keamanan, dan ketertiban umum dapat diidentifikasikan atau menunjuk pada perbuatan *cyber terrorism.* Seyogyanya jika terjadi pelanggaan terhadap ketentuan Pasal 21 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi tersebut harus disebutkan sebagai pelanggaran atau kejahatan terhadap kepentingan umum, kesusilaan, keamanan, dan ketertiban umum secara tegas, serta tersedia ancaman pidananya. Jika penyelenggara telekomunikasi dalam menjalankan

usahanya ternyata bertentangan dengan kepentingan umum, kesusilaan, keamanan dan ketertiban umum maka hendaknya ditentukan bagaimana ancaman dan sanksi pidananya, tidak hanya sebatas sanksi administrasi aja, karena kepentingan umum, kesusilaan, keamanan dan ketertiban juga memiliki kepentingan hukum yang juga harus senantiasa dilindungi dengan melalui hukum pidana.

Cyber terrorism sebagai suatu fenomena kejahatan baru di dunia maya atau sebagai satu fenomena/bentuk baru dari *cyber crime* secara umum, yang dilakukan dengan menggunakan media internet sebagai salah satu sarana telekomunikasi, merupakan salah satu perbuatan berhubungan dengan kepentingan umum, keamanan dan ketertiban umum. Hal tersebut juga dapat terlihat dalam kapasitas penyelenggara telekomunikasi, masalah telekomunikasi, alat telekomunikasi, perangkat telekomunikasi, maupun hal- hal yang memungkinkan dilakukannya perbuatan *Cyber terrorism* atau penggunaan internet sebagai salah satu sarana telekomunkasi untuk tujuan perbutan *cyber terrorism* sebagai suatu hal yang menyangkut kepentingan umum, kesusilaan, keamanan dan ketertiban umum, seharusnya juga merupakan tanggungjawab penyelenggara telekomunikasi.

Namun demikian bagi penyelenggara telekomunikasi yang melakukan kegiatan usaha penyelenggaraan telekomunikasi yang bertentangan dengan kepentingan umum, kesusilaan, ketertiban umum dan keamanan tidak ada ancaman pidananya sama sekali, melainkan hanya dikenakan sanksi administratif saja sebagaimana disebutkan dalam Pasal 45.

Hal ini akan terlihat janggal dan tidak proporsional jika dibandingkan dengan ketentuan Pasal 47 yang menyebutkan bagi mereka yang melanggar Pasal 11 ayat (1) dipidana dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak 600 juta rupiah hanya karena tidak mendapatkan izin dari menteri dalam penyelenggaraan telekomunikasi. Sementara pelanggaran atau kejahatan terhadap Pasal 21 yang menyangkut kepentingan umum, kesusilaan, keamanan dan ketertiban umum hanya dikenai sanksi administratif saja. Apakah perlu ancaman pidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp 600.000.000,- (enam ratus juta rupiah) bagi penyelenggara telekomunikasi yang tidak memenuhi kriteria Pasal 7, sementara bagi penyelenggara telekomunikasi yang melakukan kegiatan usaha penyelenggaraan telekomunikasi bertentangan dengan kepentingan umum, kesusilaan, keamanan dan ketertiban umum ternyata tidak ada ancaman pidananya sama sekali yang juga sebenarnya di dalamnya terkandung kepentingan hukum yang seyogyanya dilindungi dari sekedar penyelenggaraan telekomunikasi tanpa mendapatkan ijin dari menteri. Untuk lebih jelasnya lihat ketentuan Pasal 47, Pasal 11 dan Pasal 7 sebagai berikut:

Pasal 47: Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan / atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah).

Pasal 11: Penyelenggaraan telekomunikasi sebagaimana dimaksud dalam Pasal 7 dapat diselenggarakan setelah mendapat izin dan Menteri. Izin sebagaimana dimaksud pada ayat (1) diberikan dengan memperhatikan :

1) Tata cara yangsederhana;
2) Proses yang transparan, adil dan tidak diskriminatif; serta
3) Penyelesaian dalam waktu yang singkat.
4) Ketentuan mengenai perizinan penyelenggaraan telekomunikasi

sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dengan Peraturan Pemerintah.

Pasal 7

Penyelenggaraan telekomunikasi meliputi:

1) Penyelenggara jaringan telekomunikasi;
2) Penyelenggaraan jasa telekomunikasi;
3) Penyelenggaraan telekomunikasi khusus.

Dalam penyelenggaraan telekomunikasi, diperhatikan hal-hal sebagai berikut:

1) Melindungi kepentingan dan keamanan negara;
2) Mengantisipasi perkembangan teknologi dan tuntutan global;
3) Dilakukan secara profesional dan dapat dipertanggungjawabkan;
4) Peran serta masyarakat.

b. Sistem perumusan pertanggungjawaban pidana dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Melihat perumusan ketentuan pidana dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi sebagai mana diatur dalam Pasal 47 sampai dengan Pasal 57 maka dapat diidentifikasikan bahwa pelaku tindak pidana atau yang dapat dimintakan pertanggunjawaban pidana dalam undang-undang Telekomunikasi adalah meliputi individu/orang perorang dan korporasi. Ini terbukti dari ketentuan pasal-pasal tersebut yang diawali dengan kata "Barang siapa" dan "Penyelenggara jasa telekomunkasi", terkecuali pada Pasal 48 yang diawali dengan kata "Penyelenggaraan jaringan telekomunikasi". Masalah pertanggungjawaban pidana berkaitan erat dengan pelaku tindak pidana. Untuk pasal yang diawali dengan kata "Barang siapa", maka yang dimaksud pelaku dalam pengertian kalimat ini adalah individu dan badan hukum. Hal ini bias dilihat dalam ketentuan Pasal 1 angka 8 dan diatur lebih lanjut dalam Pasal 8 ketentuan tentang badan hukum yang disebut sebagai Penyelenggaraan jaringan telekomunikasi dan/atau penyelenggaraan jasa telekomunikasi serta Penyelenggaraan telekomunikasi khusus sebagaimana dimaksud Pasal 7 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Pasal 1 angka 8 UU No.36 tahun 1999:

Penyelenggara telekomunikasi adalah perseorangan, koperasi, badan usaha milik daerah, badan usaha milik negara, badan usaha swasta, instansi pemerintah, dan instansi pertahanan keamanan Negara

Pasal 7 ayat (1) UU No. 36 tahun 1999:

Penyelenggaraan telekomunikasi meliputi:

1) Penyelenggaraan jaringantelekomunikasi;
2) Penyelenggaraan jasa telekomunikasi;
3) Penyelenggaraan telekomunikasi khusus

Pasal 8 ayat (2) UU No. 36 tahun 1999:

1) Penyelenggaraan jaringan telekomunikasi dan/atau penyelenggaraan jasa telekomunikasi, sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf a dan huruf b, dapat dilakukan oleh badan hukum yang didirikan untuk maksud tersebut berdasarkan peraturan perundang-undangan yang berlaku,yaitu:
   a) Badan Usaha Milik Negara (BUMN);
   b) Badan Usaha MiIik Daerah (BUMD);
   c) Badan usaha swasta dan/atau Koperasi.
2) Penyelenggaraan telekomunikasi khusus sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf c dapat dilakukan oleh: Perseorangan; Instansi pemerintah; Badan hukum selain penyelenggara jaringan telekomunikasi

dan/atau penyelenggara jasa telekomunikasi.

Selain itu, dalam Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi Indonesia menyebutkan secara jelas bahwa Penyelenggaraan Jasa Telekomunikasi terdiri dari penyelenggaraan jasa telepon dasar, penyelenggaraan jasa nilai tambah telepon dan penyelengaraan jasa multimedia yang diatur lebih lanjut dalam Keputusan Menteri. Namun tidak disebutkan secara jelas apa yang termasuk dalam jasa multimedia tersebut.

Undang-Undang Telekomunikasi tidak mengatur secara lanjut dan terperinci tentang ketentuan pertanggung jawaban pidana terhadap korporasi, karena ternyata dalam undang-undang tersebut tidak membedakan pertanggung jawaban terhadap individu dan korporasi bahkan aturan pemidanaan terhadap keduanya sama. Seharusnya jika suatu undang-undang menganggap korporasi sebagai dapat dipertanggungjawabkan dalam hukum pidana maka harus dijelaskan secara rinci kapan dan siapa yang dapat dipertanggung jawabkan serta bagaimana jenis dan ancaman pidannya. Hal ini untuk menghindari berbagai kemungkinan yang dapat terjadi dalam tahap aplikasinya. Terlebih dalam haltidak dapat terbayarnya denda yang dikenakan pada korporasi, karena selama masih menggunakan KUHP maka akan dikembalikan kepada sistem induknya yaitu KUHP, di mana jika denda tidak terbayar maka akan dikenakan kurungan pengganti yang tidak mungkin dikenakan pada korporasi, apalagi dalam Undang-undang tersebut juga tidak menjelaskan yang dapat dimintakan pertanggungjawabannya dalam hal korporasi melakukan pelanggaran. Dapat disimpulkan pula bahwa dalam Undang-undang Telekomunikasi tidak ada ketentuan tentang pedoman pemidanaan atau cara bagaimana pidana tersebut dilaksanakan *(strafmodus)* sebagai pedoman bagi hakim.

c. Sistem perumusan sanksi pidana, jenis-jenis sanksi dan lamanya pidana dalam Undang-Undang Telekomunikasi

Sistem perumusan sanksi pidana dalam Undang-undang Telekomunikasi adalah alternatif kumulatif. Hal ini bisa dilihat dalam perumusannya yang menggunakan kata “dan/atau”, dengan pengecualian pada Pasal 53 yang mengancamkan sanksi pidana berupa pidana penjara secara tunggal sebagai pidana pokok yang dirumuskan secara tunggal.Jenis-jenis saksi *(strafsoort)* pidana dalam Undang-undang Telekomunikasi ini ada dua jenis yaitu pidana penjara dan denda serta tindakan yang diatur dalam Pasal 58: Alat dan perangkat telekomunikasi yang digunakan dalam tindak pidana sebagaimana dimaksud dalam Pasal 47, Pasal 48, Pasal 52, atau Pasal 56 dirampas untuk negara dan/atau dimusnahkan sesuai dengan peraturan perundang-undangan yang berlaku.

Sistem Perumusan lamanya pidana (*strafmaat*) dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi ini adalah Maksimum khusus pidana penjara berkisar antara 1 tahun sampai dengan 15 tahun. Maksimum khusus pidana denda berkisar antara Rp 100.000.000, (seratus juta rupiah) - sampai dengan Rp 600.000.000, (enam ratus juta rupiah). Selain itu disebutkan pula sanksi administratif dalam Pasal 45 dan 46 sebagai sanksi administratif yang murni dan bukan merupakan sanksi pidana administratif. Berdasarkan pembahasan di atas maka dapat diketahui bahwa Undang-Undang Nomor 36 tahun 1999, dapat digunakan untuk menanggulangi jenis tindak pidana *cyber Terrrorism,* sebagai suatu fenomena/bentuk baru *cyber crime* secara umum. Undang-undang ini menekankan pada pengaturan jaringan komunikasi.

4. Undang-Undang No. 15 Tahun 2003 *Jo*. Perppu No. 1 Tahun 2002 tentang Tindak PidanaTerorisme

Pada dasarnya permasalahan ini bukan permasalahan yang luar biasa dari kaca mata hukum pidana karena hukum pidana yang ada (KUHP) dapat digunakan untuk menanggulangi serta membawa para pelaku pemboman ke muka pengadilan. Tetapi dibalik permasalahan itu muncul pemberian nama atas perbuatan itu dengan sebutan "terorisme" sehingga menimbulkan persoalan hukum. Persoalan hukum yang timbul adalah bahwa perangkat hukum yang ada tidak dapat digunakan untuk menuntut para pelaku peledakan bom tersebut ke depan pengadilan, seolah-olah ada kekosongan hukum mengenai terorisme.[23]

Kepentingan hukum yang dibahayakan oleh tindakan terrorisme tidak hanya berupa jiwa dan harta benda, tetapi juga rasa takut masyarakat, kebebasan pribadi, integritas nasional, kedaulatan negara, fasilitas international, instalasi publik, lingkungan hidup, sumber daya alam nasional, serta sarana transportasi dan komunikasi. Terorisme dapat terjadi kapan saja dan dimana saja serta mempunyai jaringan yang sangat luas sehingga merupakan ancaman terhadap perdamaian dan keamanan, baik nasional maupun internasional. Berkaitan dengan permasalahan terorisme tersebut dibentuklah suatu Perpu Nomor 1 Tahun 2002 yang berlakunya tidak serta merta dan tidak secara otomatis. Sebagai pelaksana ketentuan Perpu Nomor 1 Tahun 2002, pemerintah mengerluarkan Perpu Nomor 2 Tahun 2002 tentang permberlakuan Perpu Nomor 1 Tahun 2002 pada peristiwa peledakan bom di Bali. Namun perkembanganya, saat ini Perpu Nomor 2 tahun 2002 ini dengan Undang-Undang Nomor 15 Tahun 2003 ditingkatkan menjadi undang-undang, sedangkan Perpu Nomor 2 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme ditingkatkan menjadi Undang-Undang Nomor 5 Tahun 2018 (selanjutnya disingkat UU terorisme).

a. Sistem perumusan tindak pidana dalam UU Tindak Pidana Terorisme

Ketentuan pidana dalam Undang-Undang Nomor 5 tahun 2018 tentang Perubahan Undang-Undang Nomor 15 tahun 2003 *Jo*. Perpu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme terdapat dalam Bab III Pasal 1 sampai dengan Pasal 19, berikut beberapa perumusan pasal dan ketentuan pidana tersebut :

Pasal 1: Ancaman Kekerasan adalah setiap perbuatan secara melawan hukum berupa ucapan, tulisan, gambar, simbol, atau gerakan tubuh, baik dengan maupun tanpa menggunakan sarana dalam bentuk elektronik atau non elektronik yang dapat menimbulkan rasa takut terhadap orang atau masyarakat secara luas atau mengekang kebebasan hakiki seseorang atau masyarakat.

Pasal 6 Setiap orang yang dengan sengaja menggunakan kekerasan atau ancaman kekerasan menimbulkan suasana teror atau rasa takut terhadap orang secara meluas atau menimbulkan korban yang bersifat massal, dengan cara merampas kemerdekaan atau hilangnya nyawa dan harta benda orang lain, atau mengakibatkan kerusakan atau kehancuran terhadap obyek-obyek vital yang strategis atau lingkungan hidup atau fasilitas publik atau fasilitas internasional, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 4 (empat) tahun dan paling lama 20 (dua puluh) tahun.

Pasal 9: Setiap orang yang secara melawan hukum memasukkan ke Indonesia, membuat, menerima, mencoba memperoleh, menyerahkan atau mencoba menyerahkan, menguasai, membawa, mempunyai persediaan padanya atau mempunyai dalam miliknya, menyimpan, mengangkut, menyembunyikan,

[23] Nyoman Serikat Putra Jaya, *Beberapa Pemikiran Ke Arah Pengembangan Hukum Pidana*, (Bandung: PT. Citra Adtya Bakti, 2008).

mempergunakan, atau mengeluarkan ke dan/atau dari Indonesia sesuatu senjata api, amunisi, atau sesuatu bahan peledak dan bahan-bahan lainnya yang berbahaya dengan maksud untuk melakukan tindak pidana terorisme, dipidana dengan pidana mati atau penjara seumur hidup atau pidana penjara paling singkat 3 (tiga) tahun dan paling lama 20 (dua puluh) tahun.

Pasal 11: Dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 15 (lima belas) tahun, setiap orang yang dengan sengaja menyediakan atau mengumpulkan dana dengan tujuan akan digunakan atau patut diketahuinya akan digunakan sebagian atau seluruhnya untuk melakukan tindak pidana terorisme sebagaimana dimaksud dalam Pasal 6, Pasal 7, Pasal 8, Pasal 9, dan Pasal 10.

Pasal l2A: Setiap Orang yang dengan maksud melakukan Tindak Pidana Terorisme di wilayah Negara Kesatuan Republik Indonesia atau di negara lain, merencanakan, menggerakkan, atau mengorganisasikan Tindak Pidana Terorisme dengan orang yang berada di dalam negeri dan/ atau di luar negeri atau negara asing dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling Lama 12 (dua belas) tahun. Setiap Orang yang dengan sengaja menjadi anggota atau merekrut orang untuk menjadi anggota Korporasi yang ditetapkan dan/atau diputuskan pengadilan sebagai organisasi Terorisme dipidana dengan pidana penjara paling singkat 2 (dua) tahun dan paling lama 7 (tujuh) tahun. Pendiri, pemimpin, pengurus, atau orang yang rnengendalikan Korporasi sebagairnana dimaksud pada ayat (2) dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 12 (dua belas) tahun.

Pasal 12B ayat (3): Setiap Orang yang dengan sengaja membuat, mengumpulkan, dan/atau menyebarluaskan tulisan atau dokumen, baik elektronik maupun nonelektronik untuk digunakan dalam pelatihan sebagaimana dimaksud pada ayat (1) dipidana dengan pidana penjara paling singkat 3 (tiga) tahun dan paling lama 12 (dua belas) tahun.

Pasal 13A: Setiap Orang yang memiliki hubungan dengan organisasi Terorisme dan dengan sengaja menyebarkan ucapan, sikap atau perilaku, tulisan, atau tampilan dengan tujuan untuk menghasut orang atau kelompok orang untuk melakukan Kekerasan atau Ancaman Kekerasan yang dapat mengakibatkan Tindak Pidana Terorisme dipidana dengan pidana penjara paling lama 5 (lima) tahun.

Pasal 14: Setiap orang yang merencanakan dan/atau menggerakkan orang lain untuk melakukan tindak pidana terorisme sebagaimana dimaksud dalam Pasal 6, Pasal 7, Pasal 8, Pasal 9, Pasal 10, Pasal 11, dan Pasal 12 dipidana dengan pidana mati atau pidana penjara seumur hidup.

Pasal 15: Setiap orang yang melakukan permufakatan jahat, percobaan, atau pembantuan untuk melakukan tindak pidana terorisme sebagaimana dimaksud dalam Pasal 6, Pasal 7, Pasal 8, Pasal 9, Pasal 10, Pasal 11, dan Pasal 12 dipidana dengan pidana yang sama sebagai pelaku tindak pidananya.

Pasal 17

1) Dalam hal tindak pidana terorisme dilakukan oleh atau atas nama suatu korporasi, maka tuntutan dan penjatuhan pidana dilakukan terhadap korporasi dan/atau pengurusnya.
2) Tindak pidana terorisme dilakukan oleh korporasi apabila tindak pidana tersebut dilakukan oleh orang-orang baik berdasarkan hubungan kerja maupun hubungan lain, bertindak dalam lingkungan korporasi tersebut baik sendiri maupun bersama- sama.
3) Dalam hal tuntutan pidana dilakukan terhadap suatu

korporasi, maka korporasi tersebut diwakili olehpengurus.

Pasal 18:

1) Dalam hal tuntutan pidana dilakukan terhadap korporasi, maka panggilan untuk menghadap dan penyerahan surat panggilan tersebut disampaikan kepada pengurus di tempat tinggal pengurus atau di tempat pengurus berkantor.
2) Pidana pokok yang dapat dijatuhkan terhadap korporasi hanya dipidana dengan pidana denda paling banyak Rp 1.000.000.000.000- (satu triliun rupiah).
3) Korporasi yang terlibat tindak pidana terorisme dapat dibekukan atau dicabut izinnya dan dinyatakan sebagai korporasi yang terlarang.

Pasal 19:

Ketentuan mengenai penjatuhan pidana minimum khusus sebagaimana dimaksud dalam Pasal 6, Pasal 8, Pasal 9, Pasal 10, Pasal 11, Pasal 12, Pasal 13, Pasal 15, Pasal 16 dan ketentuan mengenai penjatuhan pidana mati atau pidana penjara seumur hidup sebagaimana dimaksud dalam Pasal 14, tidak berlaku untuk pelaku tindak pidana terorisme yang berusia di bawah 18 (delapan belas) tahun.

Melihat berbagai ketentuan yang telah dikriminalisasikan dalam Undang-undang Pemberantasan Tindak Pidana Terorisme tersebut, nampak adanya kriminalisasi terhadap perbuatan-perbuatan yang berhubungan dengan penyalahgunaan penggunaan internet, yang berbentuk tindak pidana *cyber terrorism*. Bahkan jika dicermati dari kasus yang telah terjadi, seperti kasus ditemukannya situs yang dibuat oleh Agung Prabowo dan Agung Setyadi kaki tangan Imam Samudera dijatuhi hukuman dengan menggunakan Undang-Undang Terorisme tersebut.

b. Sistem perumusan pertanggungjawaban pidana dalam Undang-Undang Pemberantasan Tindak Pidana Terorisme.

Melihat perumusan ketentuan pidana dalam Undang-Undang Terorisme sebagai mana diatur dalam Pasal 6 sampai dengan Pasal 19 maka dapat diidentifikasikan bahwa pelaku tindak pidana atau yang dapat dimintakan pertanggunjawaban pidana dalam undang-undang pemberantasan tindap adalah meliputi individu dan korporasi. Ini terbukti dari ketentuan pasal-pasal tersebut yang diawali dengan kata "Setiap orang" dan "Korporasi". Di dalam Undang-Undang Terorisme mengatur secara lanjut dan terperinci tentang ketentuan pertanggung jawaban pidana terhadap korporasi. Hal tersebut dapat terlihat dalam Pasal 17 dan Pasal 18, yaitu:

Pasal 17:

1) Dalam hal tindak pidana terorisme dilakukan oleh atau atas nama suatu korporasi, maka tuntutan dan penjatuhan pidana dilakukan terhadap korporasi dan/atau pengurusnya.
2) Tindak pidana terorisme dilakukan oleh korporasi apabila tindak pidana tersebut dilakukan oleh orang-orang baik berdasarkan hubungan kerja maupun hubungan lain, bertindak dalam lingkungan korporasi tersebut baik sendiri maupun bersama-sama.
3) Dalam hal tuntutan pidana dilakukan terhadap suatu korporasi, maka korporasi tersebut diwakili oleh pengurus.

c. Sistem Perumusan Sanksi Pidana, Jenis-Jenis Sanksi dan Lamanya Pidana Dalam UU Pemberantasan Tindak Pidana Terorisme.

Sistem perumusan sanksi pidana dalam Undang-Undang Terrorime adalah tunggal. Hal ini bisa dilihat dalam perumusannya yang menggunakan kata mengancamkan sanksi pidana berupa pidana penjara secara tunggal sebagai pidana pokok yang dirumuskan secara tunggal.

Jenis-jenis saksi (*strafsoort*) pidana dalam Undang-Undang Terorisme ini ada dua jenis yaitu pidana penjara dan denda. Ketentuan yang mengatur pidana denda khusus ditujukan kepada korporasi, di atur dalam Pasal 18, yang menyebutkan:

1) Dalam hal tuntutan pidana dilakukan terhadap korporasi, maka panggilan untuk menghadap dan penyerahan surat panggilan tersebut disampaikan kepada pengurus di tempat tinggal pengurus atau di tempat pengurus berkantor.
2) Pidana pokok yang dapat dijatuhkan terhadap korporasi hanya dipidana dengan pidana denda paling banyak Rp 1.000.000.000.000,- (satu triliun rupiah).
3) Korporasi yang terlibat tindak pidana terorisme dapat dibekukan atau dicabut izinnya dan dinyatakan sebagai korporasi yang terlarang.

Sistem Perumusan lamanya pidana (*strafmaat*) dalam UU Terorisme ini adalah:

1) Maksimum khusus pidana penjara berkisar sampai dengan 15 tahun.
2) Maximum umum pidana penjara 15 tahun.
3) Pidana denda yang hanya ditujukan kepada korporasi sebesar Rp 1.000.000.000.000,- (satu triliun rupiah).

Berdasarkan pembahasan di atas maka dapat diketahui bahwa Undang-Undang Nomor 15 Tahun 2003 *Jo*. Perpu Nomor 1 Tahun 2002, dapat digunakan untuk menanggulangi jenis tindak pidana *cyber terrorism* sebagai suatu fenomena atau bentuk baru *cyber crime*. Hal tersebut dapat terlihat dalam ketentuan yang ada dalam Pasal 27 yang mengakui adanya *Electronic Record* sebagai alat bukti.

Cyber terrorism tidak diatur dalam berbagai Peraturan Perundang-Undangan di Indonesia. *Cyber terrorism* merupakan serangan atau ancaman secara melawan hukum terhadap komputer, jaringan komputer, dan data yang tersimpan dalam jaringan tersebut, yang memiliki tujuan untuk mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik atau sosial tertentu. Unsur melawan hukum dalam pengertian tersebut dilakukan dengan perbuatan seperti ancaman atau serangan terhadap komputer, jaringan komputer, dan data yang tersimpan dalam jaringan tersebut, sehingga akibat dari melawan hukum ini menciptakan ketakutan atau merusak infrastruktur dan kehidupan manusia.

Dalam keadaan seperti ini, pelaku tindak pidana *cyber terrorism* dapat dinyatakan bebas dari pidana karena tidak terdapat unsur melawan hukum yang diatur dalam Undang-Undang yang melekat pada perbuatannya tersebut. Oleh karena itu, untuk dapat dijatuhi suatu pidana, maka tindak pidana *cyber terrorism* harus dirumuskan secara jelas dalam Undang-Undang. Unsur melawan hukum dalam tindak pidana *cyber terrorism* tersebut berkaitan dengan asas legalitas karena tidak ada rumusan delik yang mengatur unsur melawan hukum dalam tindak pidana *cyber terrorism*. Sesuai dengan Pasal 1 Ayat (1) KUHP, sebagaimana dikenal sebagai asas legalitas.

B. Perbandingan Pengaturan *Cyber Terrorism* Di Beberapa Negara

Untuk mengantisipasi perbuatan *cyber terrorism* di Indonesia, seyogyanya para legislator juga melakukan perbandingan dengan negara lain yang telah terlebih dahulu memiliki peraturan yang berkaitan dengan penggunaan tekhnologi informasi dengan melihat berbagai aturan asing yang mengatur perbuatan *cyber crime* sebagai suatu perbuatan penyalahgunaan internet untuk tujuan perbuatan *cyber terrorism*.

Indonesia dapat mengikuti perkembangan munculnya berbagai jenis kejahatan tekhnologi informasi serta merupakan salah satu upaya harmonisasi eksternal. Perkembangan hukum di negara

lain terhadap efek negatif dari kontent internet telah melahirkan perdebatan antara pemerintah dan pengguna jasa internet tentang pengaturan kontent internet (*Internet content regulations*). Setelah dikaji, belum ditemukan negara yang mencantumkan *cyber terrorism* sebagai satu tindak pidana secara khusus. Formulasi kejahatan *cyber terrorism* hanya dimasukan dalam pengaturan mengenai *cyber crime*. Kejahatan *cyber terrorism* pun pada umumnya merupakan bagian dari *cyber crime*. Untuk jelasnya akan disajikan berbagai pengaturan kejahatan *cyber terrorism* di berbagai negara asing.

Namun demikian, dengan melakukan perbandingan hukum tidak berarti Indonesia harus menyusun Undang-undang yang sama dengan salah satu negara tersebut, seyogyanya perumus kebijakan legislatif di Indonesia dapat melakukan pilihan sesuai dengan perkembangan nilai budayanya. Penyusunan undang-undang harus tetap memperhatikan nilai-nilai sosial budaya bangsa, sebagaimana hal tersebut telah dilakukan pula oleh konsep. Soerjono Soekanto mengemukakan perbandingan hukum mungkin diterapkan dengan memakai unsur-unsur sistem hukum sebagai titik tolak perbandingan, sistem hukum mencakup tiga unsur pokok, yaitu:[24]

1. Struktur hukum yang mencakup lembaga-lembaga hukum;
2. Substansi hukum yang mencakup perangkat kaidah atau perilaku teratur, dan
3. Budaya hukum yang mencakup perangkat nilai-nilai yang dianut.

Menurut Soerjono Soekanto, perbandingan dapat dilakukan terhadap masing-masing unsur atau dilakukan secara kumulatif terhadap semuanya. Dengan metode perbandingan hukum dapat dilakukan penelitian terhadap perbagai subsistem hukum yang berlaku di suatu masyarakat tertentu atau secara lintas sektoral terhadap sistem-sistem hukum perbagai masyarakat yang berbeda-beda.

Computer Crime Research Center (CCRC) menyatakan bahwa *cyber terrorism* diartikan sebagai suatu tindakan direncanakan terlebih dahulu, bermotivasi politik serangan terhadap informasi, sistem komputer, program komputer, dan data yang mengakibatkan kekerasan terhadap sasaran oleh kelompok atau sub-nasional agen rahasia. Sejak saat itu kata *cyber terorisme* telah dimasukkan ke dalam kamus IT pakar keamanan dan teroris ahli dan daftar kata media massa profesional, sehingga pengaturan *cyber terrorism* masuk dalam pengaturan penyalahgunaan internet *(cyber crime)*.

Berikut adalah pengaturan dalam undang-undang beberapa negara asing yang mengatur delik *cyber crime* yang erat kaitannya dengan *cyber terrorism* sebagai suatu perbuatan penyalahgunaan internet.

1. Singapura

   Penggunaan media internet oleh para teroris di Asia Tenggara menunjukan peningkatan yang signifikan, kelompok yang sering dituding oleh dunia barat sebagai ekstrimis itu menggunakan ranah maya untuk menyebarkan ide radikal, merekut serta melatih para anggotanya. Temuan yang dilakukan oleh Sekolah Internasional S Rajaratnam Singapura dan Institut Strategi Kepolisian Australian memberitahu kalau, banyak pihak keamanan di Asia Tenggara yang sukses bisa mendeteksi keberadaan sebuah bom, tapi mereka tidak mengerti bagaimana bom itu dibuat. Indikasi yang menunjukan kalau peningkatan ini terjadi salah satunya adalah, makin banyaknya kelompok ekstrimis mengunggah video melalui internet mengenai cara membuat dan menggunakan bom. Menurut data yang mereka himpun, hingga 2008 lalu sudah ada 117 situs tentang kelompok radikal ini. Padahal, pada 2007 sebelumnya, situs seperti ini hanya berjumlah tidak kurang dari 15

[24] Barda Nawawi Arief, *Perbandingan Hukum Pidana*, (Jakarta: Raja Grafindo Persada, 1998), hal. 11.

saja. Dan kebanyakan dari situs tersebut, berbasis di Indonesia dan Filipiina Kita harus memperhatikan dengan serius pertumbuhan dan pergerakan kelompok radikal online tersebut.[25]

Di Singapura pengaturan mengenai penyalahgunaan internet/ *computer crime* yang mengarah kepada tindak pidana *cyber terrorism* di atur khusus di dalam undang-undang di luar KUHP nya. Beberapa ketentuan dalam perundang-undangan Negara Singapura berkaitan dengan perbuatan *cyber terrorism.*

Dari ketentuan di atas dapat disimpulkan bahwa setiap orang yang mengakses komputer yang tanpa hak/secara illegal yang dapat mengarah kepada perbuatan *cyber terrorism* 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

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 terrorism* ditambahkan pasal baru dalam KUHP Belgia yang berlaku efektif tanggal 13 2001. Bentuk *cyber terrorism* yang diatur yaitu mengenai aksi kejahatan *Hacking.*

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.

C. Penegakan Hukum Dalam Penanggulangan Tindak Pidana *Cyber Terrorism* Menurut Hukum Positif Indonesia

Untuk mengetahui terjadinya tindak pidana *cyber terrorism*, maka penulis untuk mendeskripsikan 2 studi kasus;

1. Kasus Andi Warman

Dalam Putusan Pengadilan Negeri Muaro kelas II No.91/Pid.sus/2018/PN.Mrj (Informasi dan Transaksi Elektronik) yang mengadili perkara pidana khusus dengan acara pemeriksaan biasa pada pengadilan tingkat pertama, menjatuhkan putusan sebagai berikut dalam perkara atas nama terdakwa Andi Warman berumur 20 tahun, bekerja sebagai petani dan bertempat tinggal di Kecamatan Asam Jujuhan Kabupaten Dharmasraya.

Bahwa terdakwa diajukan ke persidangan dengan dakwaan yang pada pokoknya sebagai berikut: Bahwa pada waktu dan tempat sebagaimana tersebut diatas cara terdakwa menuliskan komen atau postingan kata–kata pada akun *facebook* (fb) milik terdakwa yakni dengan cara; pertama terdakwa membuka akun facebook miliknya dengan nama Bang Andi dengan menggunakan handphone Advan seri S4E Warna putih hitam lalu terdakwa melihat postingan status Bhang Goo yang menampilkan gambar masyarakat Lubuk Besar Kecamatan Asam Jujuhan Kabupaten Dharmasraya sedang melakukan demo di beranda *Facebook* karena melihat postingan tersebut lalu terdakwa berkomentar di status

[25] *http://techno.okezone.com/index.php/ReadStory/2009/04/20/55/212093/makin-canggih-terorisasia-tenggara-gunakan-internet/makin-canggih-teroris-asia-tenggara-gunakan-internet,* Diupload Pada Tanggal 25 Februari 2021 Pukul 10.35 WIB.

Bhang Goo dan saling membalas komentar dipostingan Bhang Goo, komen yang terdakwa buat diantaranya menuliskan dan membuat kata–kata "betul sekali tu Bg go..tka PKI ", "Bsok2 kalau terulang lg kita bom aja pbrik tka" dan "kalo pak dedi lh terpecat baru dusun lubuk besar merdeka" lalu terdakwa kirimkan ke status Bhang Goo.

Adapun postingan/kata-kata yang dikirimkan oleh terdakwa pada akun Bhang Goo tersebut adalah:

1) Pada tanggal 17 Februari 2016 sekira pukul 21.53 "betul sekali tu Bg go..tka PKI". Pada tanggal 17 Februari 2016 sekira pukul 21.57 "Besok2 kalau terulang lg kita bom aja pbrik tka".
2) Pada tanggal 17 Februari 2016 sekira pukul 22.05 "kalo pak dedi lh terpecat baru dusun lubuk besar merdeka".

Bahwa dalam berkomunikasi melalui media internet terdakwa mempunyai email dari nomor Hp (085767983667), 085374741304 untuk akun media social *Facebook* terdakwa Bang Andi akan tetapi sekarang nama akun sudah terdakwa rubah dengan AD'ANDHEA dan untuk saat ini terdakwa menggunakan email dengan nomor Hp 085763607718 untuk akun *Facebook* "Andi law" dan terdakwa menggunakan whatapps dengan nomor Hp 085763209262.

Bahwa Dedi Suprianto selaku Kepala Pengamanan PT. Tidar Kerinci Agung (TKA) mengetahui postingan yang dibuat oleh terdakwa di *Facebook* pada hari Jumat tanggal 19 Februari 2016 sekira pukul 14.00 WIB, dimana sebelumnya pada hari Rabu tanggal 17 Februari 2016 ada demontrasi yang dilakukan oleh masyarakat lubuk Besar di lingkungan PT. TKA. Dedi Suprianto mengetahui postingan yang dibuat terdakwa ketika membuka akun *Facebook* miliknya kemudian membuka halaman fb atas nama Arief Toorobby dan Dedi Suprianto menemukan kata-kata "betul sekali tu Bg go. tka PKI", "Bsok2 kalau terulang lg kita bom aja pbrik tka" dan "kalo pak dedi lh terpecat baru dusun lubuk besar merdeka" dengan akun fb atas nama Bang Andi.

Bahwa berdasarkan informasi dari Arief Wibowo selaku anggota keamanan PT. TKA dan yang memiliki pertemanan di akun fb Arief Toorobby dan Bang Andi serta kenal didunia nyata menerangkan bahwa berdasarkan profil foto akun Bang Andi yang merupakan pemilik akun Bang Andi tersebut adalah terdakwa Andi Warman yang bekerja sebagai harian lepas di PT. TKA.

Perbuatan terdakwa Andi Warman sebagaimana diatur dan diancam pidana dalam Pasal 29 Undang–Undang Republik Indonesia Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik Juncto Pasal 45B Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Perkara Muhammad Bahrun Naim Anggih Tamtomo atau Bahrun Naim

Bahrun Naim merupakan dalang serangan teror bom di kawasan Sarinah. Bahrun, yang saat ini diduga berada di Suriah, dikenal sebagai ahli komputer. Naim lahir di Pekalongan pada 6 September 1983 dan besar di Pasar Kliwon. Dia diterima pada tahun 2002 dan lulus dengan gelar Associate di bidang Teknologi Informasi setelah itu dia bekerja di sebuah kafe Internet sebagai teknisi computer. Saat itu, dia sempat bertemu dengan Purnomo Putro yang menitipkan ratusan amunisi kepadanya. Purnomo merupakan buron kasus terorisme yang diduga masuk jaringan Cirebon. Setelah berbisnis warnet, Bahrun menekuni bisnis jual-beli secara *online*, beli barang di luar negeri dan menjualnya di Solo.

Pada 2010, Bahrun ditangkap Detasemen Khusus 88 Antiteror di jalan saat pulang darikantor pos untuk mengambil kiriman. Peluru titipan dari kawannya yang sudah bertahun-

tahun disimpan itu disita. Ia divonis dua setengah tahun penjara oleh Pengadilan Negeri Surakarta dengan vonis melanggar Undang-Undang Darurat No. 12 Tahun 1951 tentang kepemilikan senjata api dan bahan peledak.[26] Seusai bebas, Bahrun pergi ke Suriah untuk bergabung dengan ISIS. Di sana, Bahrun aktif menulis di blog dan berinteraksi melalui media sosial.[27] Dia juga dikabarkan membawa kabur seorang mahasiswi Universitas Muhammadiyah Surakarta, Siti Lestari (23), ke Suriah.

Bahrun Naim pergi ke Suriah untuk bergabung dengan Negara Islam Irak dan Levant (ISIS) pada tahun 2014 dan saat ini diperkirakan masih berada di Suriah. Awalnya, ia bergabung dengan kelompok pendukung ISIS di Solo.[28] Di Suriah, Bahrun membuat blog, bahrunnaimdotco, dan mulai menulis serta berinteraksi dengan pendukungnya melalui media online. Dalam salah satu postingannya. Sejak sekitar Oktober hingga November 2015, sebuah akun Facebook bernama "Muhammad Bahrunnaim Anggih Tamtomo" secara aktif membagikan tutorial membuat bom dan senjata api rakitan. Alamat lamannya pernah ditautkan ke situs web radikal lain, yang mencantumkan pembuatan bom yang lebih komprehensif.

Selama berada di Suriah, Bahrun Naim sering menggunakan internet dan menulis di blog tentang propaganda terorisme dan dan cara-cara membuat bahan peledak. Tulisan-tulisan yang ada di blog Bahrun Naim juga mengulas tentang kejadian-kejadian teror baik yang ada diluar negeri seperti kejadian di Paris dan kejadian-kejadian teror yang ada di Indonesia. selain blog, Bahrun Naim juga menggunakan media sosial lain seperti Facebook dan Telelegram untuk berkomunikasi dan memberikan informasi serta perintah untuk melakukan aksi terorisme di Indonesia. Blog Bahrun Naim yang berisi tentang propaganda dan pernah secara aktif membagikan turorial membuat bom hingga senjata api rakitan. Postingan itu, kemudian ditautkan dengan salah satu website yang belakangan sudah diblokir.

Di akun facebook yang sama, akun ini pernah membuat status bernama ultimatum yang ditujukan kepada pemerintahan Indonesia:[29] "Pesan dari komandan. Komandan udah menyerukan pertaubatan, maka langkah selanjutnya adalah terserah anda...Kepada para pejabat pemerintah Indonesia ! Bertaubatlah, kembalikan Hak Allah yang telah kalian rampas", demikian tulisan yang dibuat akun Bahrun Naim pada tanggal 22 November 2015 lalu.

Selain di akun Facebook dan website tersebut, ternyata masih ada akun Google+ dengan nama yang sama, serta masih ada website dengan nama dan isi yang nyaris serupa dengan website yang sudah diblokir sebelumnya.

Analisis Penegakan Hukum Dalam Penanggulangan Tindak Pidana *Cyber Terrorism* Menurut Hukum Positif Indonesia

Penegakan Hukum Dalam Penanggulangan Tindak Pidana *Cyber Terrorism* dalam 2 contoh kasus di atas menurut penulis belum adanya payung hukum dalam penegakan Tindak Pidana *Cyber Terrorism*. Pertama dalam Putusan Pengadilan Negeri Muaro kelas II No.91/Pid.sus/2018/PN.Mrj perkara atas nama terdakwa Andi Warman yang diancam pidana melanggar ketentuan Pasal 29 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Juncto Pasal 45B Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang

[26] "Akun Facebook Bahrun Naim Pernah Sebar Tutorial Membuat Bom !". Tribun. 14 January 2016. Retrieved January 14, 2016.

[27] Merekrut Isis dari Balik Jeruji. News Detik, January 14, 2016.

[28] CNN, "Tentang Bahrun Naim yang Diduga Sosok Pengendali" bisa ditelusuri di Wikipedia, Indonesia 26 January 2016.

[29] Krisdinar, Mona, dalam artikelnya "Bahrun Naim" Pernah sebar tutorial membuat bom", Tribun Jogja, Kamis 16 January 2016.

Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Melihat kepada unsur delik materil menimbulkan akibat tertentu, disebut dengan akibat yang dilarang atau akibat konstitutif. Titik beratnya larangan adalah pada menimbulkan akibat, sedangkan wujud perbuatan apa yang menimbulkan akibat itu tidak menjadi persoalan.

Peretasan yang dilakukan Bahrun Naim ini merupakan aib bagi aparat keamanan Indonesia. Sebab data ini ia rilis pada Agustus 2016 saat dirinya sudah populer dan masuk dalam daftar pencarian orang karena diduga jadi dalang aksi Bom Thamrin yang meledak enam bulan sebelumnya. Apa yang dilakukan Naim dengan situs BNPT sebetulnya amat mudah. Ia mengeksplorasinya dengan teknik *Google Dork*. Dalam beberapa tulisan di Telegram, Naim memposisikan diri sebagai ahli peledak. Tidak hanya mengajarkan bom berdaya ledak tinggi seperti RDX, TATP atau bom panci, ia pun mengajarkan cara membikin peledak dari bahan mudah didapat seperti bola ping pong, thinner, obat-obatan seperti aspirin, gula cangkang telur dan cuka. Sama seperti kakak-kakaknya, Ali Fauzi merupakan ahli bom organisasi Jamaah Islamiyah, ia sempat dididik Taliban di Afghanistan saat perang melawan Soviet 1990-an. Keahliannya ini membuat ia jadi pengajar di Kamp Abu Bakar, Mindanao, Filipina Selatan. Kini ia dirangkul pemerintah untuk memerangi radikalisme. Pelaku kejahatan terorisme Bahrun Naim yang melakukan propaganda dan penyebaran ideologi terorisme dengan menggunakan media internet sampai saat ini belum dapat ditangkap karena keberadaannya masih berada di negara Suriah dikabarkan sudah meninggal karena perang bersama ISIS di Suriyah pada tahun 2017.

Upaya Penanggulangan *Cyber terorisme* melalui media internet oleh Bahrun Naim dilakukan melalui penindakan hukum dan pencegahan penyebaran propaganda dengan melibatkan Badan Nasional Penanggulangan Terorisme (BNPT) sebagai koordinator, Polri dan Kementrian Komunikasi dan Informatika.

a. Penegakan Hukum

Dalam penegakan hukum terhadap pelaku kejahatan ini dilakukan oleh Polri sebagai ujung tombak dalam melakukan penindakan. Dalam menindak suatu perbuatan apalagi menjatuhkan hukum kepada pelakunya, dibutuhkan ketentuan perundangan yang lebih dahulu mengaturnya, sebagaimana yang terkandung dalam asas legalitas atau dikenal juga sebagai asas kepastian hukum. Von Feurbach menyatakan dalam adagium yang sangat terkenal, "*Nullum Delictum, nulla poena sine praevia lege poenali*", yang berarti "tiada delik, tiada pidana tanpa terlebih dahulu diatur dalam undang-undang".

Dalam penanganan kasus ini perlu dicatat bahwa payung hukum penberantasan terorisme dan tindak pidana ITE, merupakan UU khusus yang memiliki ranah pengaturan yang berbeda. Perbedaan ini cukup signifikan, terutama dalam penerapan hukum acara yang berlaku dalam hal terjadi suatu tindak pidana. Perbedaan ini diantaranya menyangkut, jangka waktu penahanan untuk kepentingan penyidikan dan penuntutan yang bisa mencapai enam bulan, kemudian tata cara intersepsi yang sempat diatur dalam Pasal 31 ayat (4) UU No. 11 Tahun 2008 yang semula mendelegasikan kepada peraturan pemerintah mengenai tata cara intersepsi, telah dinyatakan tidak memiliki kekuatan hukum yang mengikat oleh Mahkamah Konstitusi (MK). Dalam hal ini MK berpegangan kepada Pasal 28 J ayat (2) UUD 1945 yang berbunyi: Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan dan penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis.

b. Pencegahan

Dalam melakukan penanggulangan terorisme melalui media internet atau *cyber terrorism*, pemerintah melalui BNPT, Polri dan Kementerian Komunikasi dan Informatika melakukan beberapa upaya antara lain yaitu:

1) Melakukan pemblokiran terhadap situs-situs di internet yang berkaitan dengan blog milik Bahrun Naim dan situs-situs radikal yang mengandung propaganda terorisme.

2) Melakukan pengawasan (*monitoring*), pemetaan, dan perlawanan narasi dan konten radikal terorisme (kontra propaganda) terhadap situs, blog, media sosial, dan platform media online lainnya dari kelompok radikal teroris.[30]

Penggunaan media (*channel*) sebagai instrument desiminasi kontranarasi. Dalam hal ini dibutuhkan suatu media khusus yang ditujukan untuk melawan kontra-propaganda yang disebarkan oleh Bahrun Naim dan kelompok radikal lainnya. Pemberdayaan penyampaian pesan (*messenger*) yang kredibel yang secara otoritas keilmuan dan ketokohan mampu diakui masyarakat.

Membentuk dan mengoperasikan lembaga Pusat media (*media center*) BNPT. Pusat data ini bertugas mengkoordinasikan dan mengkonsolidasikan semua program dan kegiatan pencegahan terorisme yang berbasis *media literacy* di dunia maya (deradikalisasi dunia maya).[31]

Dari beberapa upaya pencegahan di atas, diharapkan penyebaran propaganda ideologi terorisme di Indonesia oleh Bahrun Naim dapat diantisipasi dan dicegah oleh pemerintah Indonesia. Kerjasama Internasional Penanggulangan Propaganda Ideologi Terorisme Melaui Media Internet.

Dalam penanggulangan propaganda terorisme melalui media internet diperlukan kerjasama internasional karena ini merupakan kejahatan transnasional seperti yang dilakukan oleh Bahrun Naim. Bentuk kerjasama internasional dan langkah-langkah strategi yang perlu diambil antara lain:

1) *Strategi Association of Soult East Asian Nation* (ASEAN) dalam Penanggulangan Terorisme. Dalam perspektif ASEAN, penanggulangan terorisme sebagai bagian dari penanggulangan kejahatan transnasional (*transnational crime*). Pada 20 Desember 1997, dicetuskan ASEAN *Declaration on Transnational Crime* di Manila. Deklarasi tersebut mengamanatkan agar dibentuk ASEAN *Ministerial Meeting on Transnational Crime* (AMMTC) dan *Senior Official Meeting on Transnational Crime* (SOMTC). Deklarasi tersebut menegaskan agar anggota ASEAN mengambil langkah-langkah penanggulangan *transnational crime*.
2) Strategi Uni Eropa dalam Penanggulangan Pemanfaatan Internet untuk Kepentingan Teroris. Salah satu bentuk kerjasama internasional yang paling maju dalam penanganan pemanfaatan internet untuk kepentingan teroris adalah kerja sama Uni Eropa. Uni Eropa memiliki instrument hukum *cyber crime* sekaligus konvensi internasional yang pertama dalam penanganan *cyber crime* yaitu *European Convention on Cyber crime*. Konvensi ini diterima oleh *Committee of Ministers of the Council of Europe* pada tanggal 8 November 2001 dan mulai ditandatangani sejak 23 November 2001. Pada 14 September 2015, konvensi ini telah ditanda tangani oleh 54 negara, baik Negara Uni Eropa maupun bukan negara anggota Uni Eropa.
3) Kerjasama internasional dengan negara-negara tempat *server hosting* maupun penyedia jejaring sosial (Facebook, Microsoft, Twitter, Youtube, Wordpress dan Blogspot,) yang kerap digunakan oleh teroris dari Indonesia berada di luar negeri berkaitan dengan kebijakan dan terkait materi terorisme. Kerjasama *government to government* dan *government to business* dalam hal ini sangat diperlukan.

Upaya Penanggulangan Hukum Atas Tindak Pidana *Cyber Terrorism* Dalam Perspektif Kepastian Hukum

Saat ini telah dilakukan upaya oleh Kementerian Politik, dan lembaga terkait lainnya seperti Badan Nasional Penanggulangan Teroris (NCTA *National Counter Terrorism Act*) untuk melakukan

[30] Bakti, Agus Surya, *Deradikalisasi Dunia Maya*, (Jakarta: Daulat Press, 2016), hal. 149.

[31] *Ibid*, hal. 168.

revisi terhadap Undang-Undang Nomor 15 Tahun 2003 yang dalam kebutuhan terhadap penanganan tindak pidana terorisme telah berkembang dengan penggunaan alat teknologi bernama komputer, dan perilaku kejahatannya telah berubah pola dengan penyalahgunaan alat eknologi komunikasi dan informasi tersebut, hingga lahir istilah *cyber crime* dalam tindak pidana *cyber terrorism*.

Termasuk juga Basrief Arief,[32] yang menyatakan bahwa "Terorisme merupakan kejahatan luar biasa (*extra ordinary crime*) yang membutuhkan pola penanganan yang luar biasa pula (*extra ordinary measure*) yang berbeda dengan penanganan tindak pidana pada umumnya".

Maka kondisi itu melahirkan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 yang kemudian menjadi Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme, yang saat ini menjadi Undang-Undang Nomor 5 tahun 2008. Kendati demikian dengan adanya rencana melakukan amandemen itu sebaiknya dipikirkan juga adanya upaya penyusunan perundang-undangan terkait dengan *cyber terrorism* dalam pembangunan hukum nasional yaitu hadirnya *cyber law* Indonesia.

Terkait dengan pembangunan hukum nasional secara khusus mengenai *cyber law* perlu perhatian serius yang diharapkan menjadi undang-undang specialis, maka jiwa undang-undang yang akan mengatur *cyber law* mengandung *philosophy* kehidupan manusia yang adil. Untuk itu dalam pandangan pakar hukum media. menyatakan sebagai berikut:

1. Ketentuan mengenai terorisme dan undang-undang lain terkait *cyber terrorism* harus sesuai dengan budaya, kondisi masyarakat, stabilitas politik pemerintahan, struktur geografis dan asas keseimbangan antara proteksi HAM serta pembatasan HAM dalam kerangka pandangan legastik-moralistik yang menegaskan pendekatan politik.
2. Penyusunan rumusan delik harus memperhatikan kepentingan keamanan negara (*Nasional Defence*), kepentingan peradilan yang baik (*due process of law*) dan kepentingan perlindungan korban (*victim protection*).
3. Kebijakan kontra terorisme harus tetap memperhatikan mekanisme demokratis dan titik keseimbangan prinsip kebebasan dan prinsip keamanan. Ditegakannya *civil liberties* seperti tetap memperhatikan *non derogable rights*, diantaranya dengan menghormati hak untuk diperlakukan sama di depan hukum. Penghormatan terhadap hak asasi manusia merupakan salah satu syarat berdirinya negara hukum.
4. Terkait dengan kewenangan luar biasa para penegak hukum dalam menangani aksi terorisme pada umumnya dan *cyber terrorism* pada khususnya, maka perlu dipertimbangkannya penerapan *sunset principle*, yaitu pemberlakuan hukum yang bersifat time limited, khusunya bagi pasal-pasal yang dimaksudkan untuk memberi kewenangan luar biasa kepada para penegak hukum dalam mengangani aksi terorisme; perlu diperhatikan sistem peradilan pidana yang terpadu sebab proses investigasi melibatkan aparat *non-judicial* seperti Badan Intelijen Nasional (BIN) dan TNI. Selain itu, keterlibatan BIN dan TNI dalam mekanisme *pre-trial* yang diadopsi Anglo Saxon tanpa mengadopsi sistem peradilan akan mengindahkan hak-hak untuk mengajukan keberatan *(harbeas corpus)* sehingga mekanisme praperadilan tidak dapat dilakukan; perlu adanya regulasi yang rinci mengenai *code of conduct, rule of engangement* dan ketentuan pidana bagi aparat yang melakukan pelanggaran; diaturnya secara khusus mengenai hak-hak tersangka ataupun terdakwa dan dalam proses penyelidikan dan penyidikan, investigasi dan hearing harus dilakukan sesuai ketentuan Undang-Undang Nomor 5 Tahun 1998 tentang Konvensi Menentang Penyiksaan dan Perlakuan atau Penghukuman Lain Yang Kejam, Tidak Manusiawi atau Merendahkan Martabat Manusia, dimana yang melarang penyiksaan dalam proses penyidikan dan penyelidikan.

Permasalahan hukum yang ditimbulkan akibat kejahatan dunia maya (*cyber crime*) seperti *cyber terrorism*, dipandang serius untuk disikapi dengan menghadirkan undang-undang khusus diluar KUHP, seperti halnya ketentuan

[32] Kejaksaan Agung Republik Indonesia, *Panduan Penanganan Perkara Tindak Pidana Terorisme Kejaksaan Agung Republik Indonesia*, Cet ke I, 2013, hal. 5.

hukum *cyber law* yang diharapkan dapat menjamin adanya kepastian hukum dalam kejelasan tindak pidana *cyber terrorism,* prediktabilitas dan kepastin hukum dalam mengatasi persoalan *cyber terrorism*.

Sisi lain dari aspek objektif untuk mempertanggungjawabkan *Cyber Terorrism* merupakan masalah juridiksi, khususnya yang berkaitan dengan masalah ruang berlakunya hukum pidana menurut tempat. Dalam sistem hukum pidana yang berlaku saat ini, Hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas teritorial) dan untuk warga negaranya sendiri (asas personal/nasional aktif). Hanya untuk delik-delik tertentu dapat digunakan asas nasional pasif dan asas universal. Asas-asas ruang berlakunya hukum pidana menurut tempat yang konvensional/ tradisional (juridiksi fisik) itu pun tentunya menghadapai tantangan sehubungan dengan masalah pertanggungjawaban *Cyber Terrorism.*

Masalah juridiksi *Cyber Terorism* yang merupakan bagian dari jenis *cyber crime* tersebut termasuk yang sangat serius. Barbara Etter, didalam tulisannya berjudul *Critical Issues in High Tech Crime*[33] mengidentifikasi beberapa masalah kunci yang terkait atau yang menyebabkan timbulnya masalah juridiksi ini dalam konteks internasional antara lain:

1. Tidak adanya consensus global mengenai jenis-jenis CRC (*Computer Related Crime*), dan tindak pidana pada umumnya;
2. Kurangnya keahlian aparat penegak hukum dan ketidakcukupan hukum untuk melakukan investigasi dan mengakses sistem komputer.
3. Adanya sifat transnasional dan *computer crime;*
4. Ketidakharmonisan hukum acara/procedural di berbagai negara;
5. Kurang sinkronisasi mekanisme penegakan hukum, bantuan hukum, ektradisi, dan kerja sama internasional dalam melakukan investigasi *cyber crime.*

Sehubungan dengan masalah juridiksi, UU di Australia memberi kewenangan untuk menuntut seseorang di mana pun berada yang menyerang komputer diwilayah Aunstralia. Bahkan di USA, tidak hanya dapat menuntut setiap orang asing yang menyerang komputer-komputer di USA, tetapi juga orang Amerika yang menyerang komputer di Negara-negara lain.[34] Dari ketentuan demikian terlihat bahwa komputer dipandang sebagai kepentingan nasional dan sekaligus kepentingan international yang sepatutnya dilindungi, apalagi yang berkaitan dengan penyalahgunaan internet yang mengarah kepada perbuatan *Cyber Terorism,* tentunya juga akan sangat dilindungi sehingga terkesan dianut asas ubikuitas *(the principle of ubiquity)* atau asas *omnipresence* (ada dimana-mana). Dianutnya asas ini tentunya harus didukung oleh kemampuan suatu Negara dan kerjasama international.

Sehubugan dengan masalah juridiksi tersebut, dalam Konsep RUU KUHP akan ada ketentuan mengenai perluasan asas berlakunya hukum pidana dan tempat terjadinya tindak pidana yang berorientasi pada "perbuatan" dan "akibat", sehingga diharapkan dapat menjaring tindak pidana (*Cyber Terorism* yang merupakan bagian dari *crime*) di luar territorial Indonesia yang akibatnya terjadi di Indonesia.

D. Kesimpulan

1. Penegakan hukum dalam penanggulangan tindak pidana *cyber terrorism* menurut hukum positif Indonesia dalam 2 contoh perkara *cyber terrorism* belum diatur baik dalam undang-undang yang mengatur tentang *cyber* law (seperti UU ITE) dan Undang-Undang tentang terorisme. 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.
2. Ketentuan hukum penanggulangan tindak pidana *cyber terrorism* dari perspektif kepastian hukum perlu dimasukan secara khusus pengaturan tindak pidana *cyber terrorism* pada ketentuan Hukum Dunia maya (*cyber law*) sebagai *lex specialis.* Pengaturan mengenai *cyber terrorism* dalam *cyber law* diharapkan bisa

[33] Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Cyber Crime di Indonesia,* (Jakarta: PT. Raja grafindo Persada, 2005), hal. 107-108.

[34] *Ibid*, hal. 108.

memberikan kepastian hukum yang mengatur secara komprehensif pergerakan dan penggunaan serta penyimpangan dalam tindakan kejahatan *cyber* yang menggunakan komputer sebagai alat utama dan kemanfaatan dari media teknologi yang berkembang. Artinya tidak hanya bergantung pada satu Undang-Undang (*umbrella act*) saja, meski telah ada Undang-Undang Nomor 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme, ataupun Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, atau Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

E. Saran

1. Badan legislative agar mengadakan formulasi tindak pidana *cyber terrorism* dalam RUU KUHP Nasional beserta penjelasanya secara jelas dan terang sebelum disahkan dan diberlakukan, sehingga dapat mengatasi kekosongan hokum atas bentuk-bentuk kejahatan *cyber* terrorism yang mengancam keamanan setiap orang dan negara serta dapat mewujudkan kodifikasi hukum pidana nasional.
2. Pemerintah diharapkan memiliki keterbukaan informasi dalam dunia peradilan, sehingga masyarakat dapat mempelajari maupun mengkoreksi pelaksanaan hukum di pengadilan. Jadi, masyarakat mengetahui bagaimana pengadilan memutus suatu perkara khususnya kasus yang terkait dengan kemajuan teknologi dan informasi yang telah terjadi Indonesia.

DAFTAR PUSTAKA

"Akun Facebook Bahrun Naim Pernah Sebar Tutorial Membuat Bom !". Tribun. 14 January 2016. Retrieved January 14, 2016.

Agus Surya Bakti, *Deradikalisasi Nusantara, Perang Semesta Berbasis Kearifan Lokal MelawanRadikalisasi dan Terorisme*, (Jakarta: Daulat Press, 2016).

Bakti, Agus Surya, *Deradikalisasi Dunia Maya*, (Jakarta: Daulat Press, 2016), hal. 149.

Barda Nawawi Arief, *Perbandingan Hukum Pidana*, (Jakarta: Raja Grafindo Persada, 1998), hal. 11.

Barda Nawawi Arief, *Sari Kuliah Perbandingan Hukum Pidana*, (Jakarta: Raja Grafindo Persada, 2002), hal. 254-255.

Barda Nawawi Arief, *Tindak Pidana Mayantara, Perkembangan Cyber Crime di Indonesia,* (Jakarta: PT. Raja grafindo Persada, 2005), hal. 107-108.

Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia*, (Jakarta: Raja Grafindo Persada, 2006).

CNN, "Tentang Bahrun Naim yang Diduga Sosok Pengendali" bisa ditelusuri di Wikipedia, Indonesia 26 January 2016.

Eksistensi dan Perkembangan *ISIS*: Dari Irak Hingga Indonesia, Najamuddin Khairur Rijal Prodi Hubungan Internasional, Universitas Muhammadiyah Malang.

Eska Nia Sarinastiti1 dan Nabilla Kusuma Vardhani, *Internet dan Terorisme: Menguatnya Aksi Global Cyber Terrorism Melalui New Media*, Januari 2018.

H. Sutaman, *Cyber Crime, Modus Operandi dan Penangulangannya*, (Jogjakarta: LeksBang Pressindo, 2007), hal. 83.

***http//www.ParentNews Safety.com, cyber ethics: Everyone should practice responsible social and legal behavior while on the Internet. No one should participate in any form of cyber-bullying*.**

***http://techno.okezone.com/index.php/ReadStory/2009/04/20/55/212093/makin-canggih-terorisasia-tenggara-gunakan-internet/makin-canggih-teroris-asia-tenggara-gunakan-internet,* Diupload Pada Tanggal 25 Februari 2021 Pukul 10.35 WIB.**

Kejaksaan Agung Republik Indonesia, *Panduan Penanganan Perkara Tindak Pidana Terorisme Kejaksaan Agung Republik Indonesia*, Cet ke I, 2013, hal. 5.

Krisdinar, Mona, dalam artikelnya "Bahrun Naim" Pernah sebar tutorial membuat bom", Tribun Jogja, Kamis 16 January 2016.

Merekrut Isis dari Balik Jeruji. News Detik, January 14, 2016.

Muhammad Ikhlas Thamri, *Densus 88 Undercover*, (Solo: Quo Vadis, 2007), hal. 74.

Nyoman Serikat Putra Jaya, *Beberapa Pemikiran Ke Arah Pengembangan Hukum Pidana*, (Bandung: PT. Citra Adtya Bakti, 2008).

Rizky Reza Lubis Alumni Universitas Pertahanan Indonesia, Potensi Pengguna Internet Indonesia Dalam Counter-Cyber Radicalization Indonesia's Netizen Potential On Counter-Cyber Radicalization.

Sudarto, *Hukum dan Hukum Pidana*, (Bandung: Alumni, 1981), hal. 159.

Sutarman, *Cyber Crime, Modes Operandi dan Penanggulangannya*, (Jogjakarta: LaksBang Pressindo, 2007), hal. 101-102.

Ufran, *dalam journal tentang Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism,* Fakultas Hukum Universitas Mataram, Oktober 2014.

Wahyono, Edi dalam investigasi, merekrut dibalik jeruji, news, 2016.

Yusuf Qardhawi, *Fiqih Jihad: Sebuah Karya Monumental Terlengkap Tentang Jihad Menurut Al-Qur'an dan Sunnah*, (Bandung: Mizan, Cet. I, 2010), hal. 1.