Kebijakan Formulasi Hukum Pidana Tentang PenanggulanganTindak Pidana Terorisme Siber (*Cyber Terorism*) Di Indonesia

Oleh
Boby Iskandar
Dosen STIH Umel Mandiri Jayapura
Eren Arif Budiman
Dosen STIH Umel Mandiri Jayapura

Abstrak

Di indonesia cyber terorisme di atur dalam Undang-Undang Terorisme Nomor 1 Tahun 2002 , Undang-Undang ITE Nomor 19 Tahun 2016 dan peraturan Presiden Republik Indonesia Nomor 53 tahun 2017. Namun pokok perkara hukum yang sebenarnya bertumpu pada UU ITE No.19 tahun 2016 menurut hemat penulis masih banyak terdapat kelemahan yuridis dan dari formulasinya belum sistemik, karena memuat hal-hal yang bersifat umum dan belum mampu maksimal dalam menanggulangi jenis *cyber terorism* melalui sarana sistem hukum pidana dengan spesifik dan jelas, sehingga UU ITE No.19 tahun 2016 ini seringkali digunakan untuk menjerat pelaku yang semata-mata menggunakan sarana elektronik saja sehingga menimbulkan kesan ambigu dalam penerapannya karena menurut hemat penulis, seharusnya keberadaan UU ITE ini seharusnya lebih difokuskan kepada penanganan kejahatan dalam dunia siber yang didalamnya juga termasuk terorisme siber (*cyber terorism*).

A. Pendahuluan

Perkembangan pesat dalam bidang teknologi dan informasi yang semakin maju saat ini terjadi karena semakin banyak kebutuhan manusia baik itu sarana komunikasi, transportasi, dan banyak lagi hal lainnya yang berguna untuk memudahkan hidup manusia di era modern saat ini untuk membantu aktifitasnya sehari-hari. Hal ini tentu saja memacu kita untuk mengejar ketertinggalan dan dituntut untuk melek terhadap perubahan saat ini dan mendorong adanya revolusi teknologi pada abad 21, namun dibalik keberhasilan itu, ada terdapat banyak celah bagi para pelaku kejahatan juga untuk memanfaatkan teknologi untuk mewujudkan tujuannya, khususnya di bidang terorisme. Apa yang dulunya kejahatan terorisme dijalankan secara konvensional, namun saat ini kejahatan terorisme dapat dilakukan dengan memanfaatkan teknologi yang semakin canggih, sehingga dampak negatif dari aksi terorisme siber lebih parah daripada aksi terorisme konvensional, karena aksi terorisme siber bersifat massif dan terstruktur yang berdmpak secara global.

Kemajuan dunia teknologi informasi tidak terlepas dari jaringan komputer yang menghubungkan koneksi antar negara atau antar benua yang berbasis *transmission control protocol/internet protocol*. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah jaringan yang

lebih kecil yang mempunyai sistem jaringan yang berbeda-beda.[1]

Berdasarkan penelitian yang dilakukan sebelumnya oleh Sri Ayu Astuti dalam jurnal *Rechtsidee* pada tahun 2015, mengemukakan bahwa aksi terorisme yang marak belakangan ini ditenggarai merupakan hasil giat masif dari ruang cyber. Kejahatan berkaitan dengan ideologi dan pencucian otak (brain wash) mengenai paham negara dan perekrutannya dengan melakukan komunikasi aktif menggunakan alat teknologi, menjadi kegiatan utama yang digerakan oleh kepentingan kelompok radikalisasi untuk melakukan aksinya. Contoh nyata yang dapat kita lihat saat ini adalah organisasi Radikal yang dikenal dengan ISIS (Islamic State of Iraq and Syam/Syria) menggunakan jejaring media sosial untuk merekrut anggota baru dan terus secara kuat mempublikasikan keberadaan kelompoknya sebagai kekuatan negara baru yang akan memimpin kekhalifahan di muka bumi dan dengan berbagai cara melakukan aksi teror melalui dunia maya[2]

Dengan adanya internet sebagai “the network of the networks” ke seluruh dunia, membuat terciptanya suatu ruang (space) atau dunia baru, yang dinamakan Cyberspace.[3]

Cyberspace diyakini sebagai suatu bangunan atau ruang komunikasi global dimana tidak ada satu pun negara yang berhak mengatur apa saja isi informasi yang

[1] Maskun, Kejahatan Siber suatu pengantar, Jakarta, Prenada Media Grup, 2013 hal.46

[2] Sri Ayu Astuti, Penegakan Hukum Terhadap Terorisme Dunia Maya Di Indonesia, Jurnal Rechtsidee FH Universitas Muhamadiyah Sidoarjo, 2015, hlm.2

[3] Edmon Makarim,Kompilasi Hukum Telematika, Jakarta, Raja Grafindo,2005, hal.5

ingin dikomunikasikan antara dua orang atau banyak orang.[4]

Terorisme siber merupakan salah satu bentuk kejahatan cyber. Dari segi konsep, *Cyber terrorism* tidak jauh berbeda dengan terorisme yang dilakukan dengan cara konvensional / tradisional, hanya saja disini memiliki unsur "cyber". Beberapa peneliti berpendapat bahwa kegiatan terorisme di cyberspace dianggap sebagai Cyber-terrorism[5]

B. Metode Penelitian

Penelitian dalam ilmu hukum adalah keseluruhan aktifitas berdasarkan disiplin ilmiah untuk mengumpulkan, mengklasifikasikan, menganalis dan menginterpretasikan fakta serta hubungan di lapangan hukum dan di lapangan lain-lain yang relevan bagi kehidupan hukum, dan berdasarkan pengetahuan yang diperoleh dapat dikembangkan prinsip-prinsip ilmu pengetahuan dan cara-cara ilmiah untuk menanggapi berbagai fakta dan hubungan tersebut[6].

L.Morris Cohen sebagaimana yang dikutip oleh Zainuddin Ali, mendefinisikan penelitian hukum sebagai segala aktivitas seseorang untuk menjawab permasalahan hukum yang bersifat akademik dan praktis, baik yang bersifat asas-asas hukum, norma-norma hukum yang hidup dan berkembang dalam masyarakat, maupun yang

[4] Edmon Makarim, *Ibid*

[5] Zahri Yunus dan Rabiah Ahmad, A Dynamic Cyber-terrorism Framework dalam Internasional Journal of Computer Science and Information Security Vo. 10, No 2,2012. hlm. 149

[6] Teuku Muhammad Radie, Makalah:Penelitian Hukum dalam Pembinaan dan Pembaharuan HukumNasional, 1974, Jakarta: BPHN Departemen Kehakiman, hlm. 14, online pada lib.ui.id/file?file=pdf/metadata-20164472.pdf, diakses pada tanggal 25 Mei 2021

berkenaan dengan kenyataan hukum dalam masyarakat.[7]

Eksistensi rangkaian suatu metode penelitian dapat diawali dari penentuan

jenis penelitiannya, dimana jenis penelitian ini juga menggunakan Jenis penelitian yuridis normatif, yaitu penelitian terhadap asas-asas hukum dan peraturan-peraturan yang ada terkait dengan cyber-terrorism, cyber crime, dan terorisme.

Penulis juga menggunakan desain penelitian kuantitatif dengan desain deskriptif dimana tujuan dari desain ini sendiri adalah untuk menggambarkan, menjelaskan dan mendeskripsikan segala situasi, fakta dan kondisi tentang masalah yang ada secara akurat dan sistematis

Dalam melakukan penyusunan penelitian ini, penulis melakukan pengambilan data di Perpustakaan Universitas Indonesia untuk melengkapi informasi yang diperlukan, pengambilan data di Badan Nasional Penanggunggulangan Terorisme (BNPT) yang bertugas untuk penanggulangan kejahatan terorisme , Badan Siber dan Sandi Negara (BSSN) yang bertanggung jawab untuk keamanan ruang siber dan juga mengurusi masalah infrastruktur siber dan teknologinya dan Bareskrim Polri khususnya di direktorat tindak pidana siber (Dittipidsiber) yang dibentuk untuk melakukan penegakan hukum terhadap kejahatan siber. Secara umum, Dittipidsiber menangani dua

[7] Zainuddin Ali, 2010, Metode Penelitian Hukum, Jakarta: Sinar Grafika, hlm.19

kelompok kejahatan, yaitu computer crime dan computer-related crime.

C. Hasil dan Pembahasan

Secara umum yang dimaksud kejahatan komputer atau kejahatan di duniacyber (cybercrime) adalah "Upaya memasuki dan atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut[8].

Istilah cyber crime saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (cyberspace) dan tindakan kejahatan yang menggunakan komputer[9]. Barda Nawawi Arief juga merujuk pada kerangka (sistemik) Draft Convention on Cyber Crimedari Dewan Eropa (Draft No. 25, Desember 2000), yang menyamakan peristilahan antara keduanya dengan memberikan definisi *cyber crime* sebagai "*crime related to technology, computers and the internet*" atau secara sederhana berarti kejahatan yang berhubungan dengan teknologi, komputer dan internet.

Perkembangan dunia teknologi yang semakin berkembang ini merupakan fenomena munculnya kejahatan di dunia maya yang disebut *cyber crime* dimana pada dasarnya ini merupakan kejahatan tradisional yang berkembang mengikuti perkembangan teknologi juga, sehingga mengakibatkan evolusi dari jenis kejahatan yang

[8] Goodall, K. (2013). Conceptualising 'Racism' in Criminal Law. Cambridge University Legal StudieseeJournal,Vol. 33, (No 2 June). hal.9

[9] Arief, Barda N. (2005). Kebijakan Penanggulangan Cyber Crime dan Cyber Sex. Jurnal LawReform,Vol. 1, (No.1), hal 3

serupa terjadi di masa lalu. Sebagai ilustrasi, kita dapat memperhatikan gambar berikut.

(Sumber :www.quora.com)

Surface web atau yang dikenal juga dengan *Visible web* merupakan bagian dari *World Wide Web* (www) yang tersedia untuk umum dan dapat dicari dengan mesin pencari web standar. Surface Web hanya terdiri dari 10 persen dari informasi yang ada di internet. Surface Web dibuat dengan koleksi halaman Web publik di server yang dapat diakses oleh mesin pencari apa pun. *Surface web* dapat digunakan oleh semua orang untuk mengakses sosial media, belanja online, belajar, hingga bekerja. Hanya saja semua kegiatan pengguna di internet dapat dilihat oleh penyedia ISP.

*Deep Web, d*alam istilah awam *Deep Web* merupakan level yang lebih dalam dari visible web di internet. *Deep Web* merujuk kepada situs web yang tidak bisa diakses dengan mudah melalui mesin pencari konvensional seperti Google atau Yahoo. Hal ini dikarenakan konten yang ada pada *Deep Web* belum diindeks oleh mesin pencari umum yang digunakan. Bisa dikatakan, jika sebuah situs web tidak diindeks oleh mesin pencari situs, maka alamat itu hanya dapat diakses dengan menavigasi langsung ke URL melalui tautan atau mengetikkan alamat web yang tepat di browser web. Banyak situs web yang menggunakan Deep Web karena alasan informasi yang mereka miliki tidak dimaksudkan

untuk konsumsi publik. Pemilik konten membuat informasi tersebut tidak dapat diakses dengan memastikan tidak muncul dalam hasil pencarian browser internet. Perlu dicatat bahwa *Deep Web* tidak selalu ilegal dan ada banyak kegiatan yang terjadi yang sepenuhnya dalam konteks hukum. Banyak pengguna yang menggunakan *Deep Web* sebagai salah satu situs web yang mengizinkan penggunaan dan komunikasi secara anonim dan pribadi. *Deep Web* juga digunakan oleh para junalis, whistleblowers (pelapor), pengunjuk rasa, kelompok advokasi anti sensor, hingga masyarakat yang ditindas oleh rezim politik.

Dalam Deep Web terdapat bagian khusus yang tersembunyi dan berisi sejumlah besar data dan informasi yang sangat sensitif, rahasia, dan juga penting, seperti:

- Situs internal perusahaan besar, asosiasi, dan organisasi perdagangan.
- Sistem intranet sekolah, perguruan tinggi, dan universitas.
- Akses ke database online.
- Situs web yang dilindungi password dengan akses hanya anggota
- Halaman enshrouded Paywall.
- Halaman akses berjangka waktu seperti yang ditemukan di situs pengambilan tes online.
- Mengurangi paywalls untuk konten digital yang diblokir.
- Akun pribadi seseorang untuk media sosial, email, perbankan, dan lainnya.

Dark Web atau yang lebih dikenal dengan *Dark Net* merupakan bagian yang paling dalam di internet, lebih dalam dari *Deep web*. Untuk

mengakses *Dark Net*, diperlukan tingkat kecakapan internet tertentu, dengan langkah-langkah yang diperlukan yang harus diambil untuk tidak hanya memasuki dunia enshroud ini sambil menjaga privasi maksimal. Untuk menjaga anonimitas, pengunjung *Dark Net* biasanya menggunakan perangkat lunak anonimitas khusus seperti Tor untuk menutupi identitas mereka seperti lokasi, alamat IP, dll.

Dark Web sangat menarik bagi pengguna internet karena berbagai alasan. Sifat dan metodologi rumit yang diperlukan untuk mengakses dunia ini telah secara efektif menjadikan *Dark Net* dunia rahasia, penuh dengan kegiatan yang bersemangat, pasar gelap, pemandangan, dan fasilitas yang terbatas pada beberapa orang atau organisasi tertentu.

Dark Web secara historis hanya menjadi salah satu bagian yang diakses pengguna internet, sebesar 3 persen. Dan banyak digunakan oleh organisasi kejahatan dan perdagangan ilegal.[10]

Penulis juga telah mencoba mengkaji isi dalam *dark web*, dimana penulis juga mendapatkan bukti nyata bahwa baik barang terlarang seperti pembelian senjata, jasa pembunuh bayaran, sampai perdagangan manusia bisa di dapatkan disini denan menggunakan pembayaran melalui bitcoin atau *crypto currency* lainnya, namun saat ini lebih popular menggunakan bitcoin[11].

[10] https://cyberthreat.id/read/6226/Apa-Beda-Surface-Web-Deep-Web-dan-Dark-Web, akses 25 Mei 2021

[11] Penulis menggunakan tor onion yang dijalankan oleh system operasi linux tails 4.01 untuk mengakses sebuah situs zqktlwi4fecvo6ri.onion yang dijelaskan lebih lanjut, Sebagai layanan

Di indonesia sendiri cyber terorisme di atur dalam Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme yang telah direvisi menjadi Undang undang No. 5 Tahun 2018 tentang Perubahan atas UU No 15 Tahun 2003 dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan untuk lembaga pendukung dan pihak terkait yang ikut serta dalam penanganan segalajenis tindak pidana dan serangan cyber di Indonesia di atur dalam Peraturan Presiden Republik Indonesia Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara.

Pada Pasal 46 b Undang-undang No. 5 tahun 2018 tentang Perubahan atas Undang-undang no. 15 tahum 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-undang No. 1 tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang menyatakan bahwa semua peraturan pelaksana harus dibentuk dalam waktu 1 tahun sejak 22 Juni 2018 yakni saat undang-undang tersebut diundangkan. Namun hingga saat inI, Pemerintah baru menyelesaikan 1 buah peraturan pelaksana yaitu Peraturan Pemerintah Nomor 77 Tahun 2019 tentang Pencegahan Tindak Pidana Terorisme dan Pelindungan terhadap Penyidik, Penuntut Umum, Hakim,

tersembunyi, yang disebut dengan The Hidden Wiki. Situs ini menyediakan berbagai tautan dalam format wiki ke layanan dan situs tersembunyi lain di clearnet (situs yang hanya dapat diakses di peramban standar). Tautan-tautan tersebut ada yang mengarah ke situs berbagi pornografi anak dan situs perdagangan elektronik yang menjual barang dan jasa selundupan, termasuk senjata, uang dan dokumen identitas palsu, informasi kartu kredit curian, pembunuh bayaran, dan obat-obatan seperti Silk Road.

dan Petugas Pemasyarakatan. PP tersebut pun juga baru diundangkan pada 13 November 2019. Kesimpulannya, selama masa 1 tahun sebagaimana diamanatkan UU Terorisme, tidak ada satu produk peraturan pelaksana pun yang dibuat oleh Pemerintah maupun DPR. Padahal, masih terdapat 1 peraturan pelaksana lainnya yang terkait dengan kebijakan pidana yang juga perlu segera dibentuk, yakni tentang Pembentukan Tim Pengawas Penanggulangan Terorisme yang direncanakan dapat terlaksana pada tanggal 22 Juni 2021.[12]

Berkembangnya tindak kejahatan dari berbasis konvensional menjadi elektronik tentu sangat berbahaya, maka dari itu perlu formulasi, pencegahan, dan penanganan yang tepat dari pihak berwajib untuk menghadapi kejahatan *cyber terrorism*.

Ancaman *cyber terrorism* cepat atau lambat tidak hanya akan mempengaruhi keamanan nasional tapi juga akan mempengaruhi keamanan internasional, sangat penting bagi kita untuk mengetahui bagaimana sistim hukum mengatur mengenai *cyber terrorism*. Karena dalam kehidupan nyata, kelompok-kelompok teroris dapat melakukan hal-hal yang antara lain[13]:

- Meningkatkan publisitas dan mempperkuat propaganda

  Teroris memang memilih dan mendistribusikan informasi tindakan mereka walaupun tindakan mereka dapat dikatakan tidak umum/wajar. Seperti beberapa artikel

[12] https://www.dpr.go.id/berita/detail/id/32593/t/Legislator+Dorong+DPR+Segara+Bentuk+Tim+Pengawas+Penanggulangan+Terorisme, ases pada 25 mei 2021.

[13] https://inet.detik.com/cyberlife/d-1350189/7-ancaman-teroris-lewat-internet, akses 25 Mei 2021

menggambarkan kekerasan, seringkali dalam bentuk video dan gambar. Sebagai contoh sebuah situs menjadi pra-misi foto-foto yang dipublikasikan oleh Harimau Tamil, skuadron Tiger Air yang beberapa hari sebelumnya telah melakukan serangan udara yang sukses terhadap pemerintah Sri Lanka. Contoh yang lebih ekstrim lagi, distribusi pemenggalan wartawan Daniel Pearl oleh organisasi teroris 'Gerakan Nasional Untuk Pemulihan Kedaulatan Pakistan'.

- Data Mining

  Internet adalah sumber informasi yang sangat besar dan siapapun dapat memanfaatkan dan para teroris juga dapat menggunakannya. Menurut Menteri Pertahanan Donald Rumsfeld yang berbicara 15 Januari 2003, sebuah manual pelatihan Al-Qaeda di Afghanistan mengatakan kepada pembacanya bahwa 'Menggunakan sumber-sumber publik secara terbuka dan tanpa menggunakan cara-cara ilegal sangat mungkin untuk mengumpulkan 80% dari semua informasi yang diperlukan tentang musuh-musuh meraka.

  Internet memungkinkan akses kepada peta yang sangat rinci dan akurat, berbagai skema dan sumber data lainnya, yang memungkinkan teroris mengumpulkan informasi tersebut sebagai target yang sangat potensial. Lebih penting lagi, begitu data ini telah dikumpulkan, dikompilasi ke dalam satu buah 'volume' dan menjadi 'how' dan seolah-olah sebagai manual yang didistribusikan di antara organisasi teroris.

- Pendanaan / *funding*

Kelompok-kelompok teroris telah memanfaatkan secara penuh kemampuan internet untuk menciptakan dana, apakah dana tersebut sah atau bahkan sebaliknya. Metode utama teroris mencapai hal ini adalah dengan cara:

a. Menjual barang, barang yang secara langsung berkaitan dengan organisasi teroris seperti CD, DVD dan buku-buku organisasi tersebut.
b. Membuat Website dan email berbasis banding, yakni mengirim email ke simpatisan yang terdaftar dan tertarik pada situs web group tersebut, posting pesan di newsgroup/forum dan website mereka sendiri yang akan memberikan arah, bagaimana dan di mana sumbangan tersebut dapat didapat.
c. Deception, menggunakan amal yang tampaknya sah atau bisnis yang tidak diketahui para donaturnya dan kemudian mengarahkan dana tersebut untuk kegiatan teroris.
d. Aktivitas kriminal, yakni melakukan aktivitas tidak sah/kriminal untuk mendapatkan dana bagi kelompok teroris tersebut termasuk penipuan kartu kredit, broker online, investasi keuangan dan lainnya.

- Rekruitmen anggota

  Pada bagian ini pada dasarnya terkait dengan propaganda, organisasi teroris dapat memantau pengguna yang menelusuri web mereka, menangkap profil mereka dan informasi tentang mereka dan bila dianggap mungkin sangat berguna untuk merekrut mereka dan menghubungi mereka. Proses perekrutan dimulai dari ketika pengguna internet mulai menyerap propaganda pada website-website yang sering dikunjungi dan menarik

bagi mereka, misalnya sering dibahas tentang 'karismatik' gaya penyampaian yang disampaikan 'Osama Bin Laden' melalui pesan-pesan video.

Mungkin didorong oleh video ini, pengguna internet mencari jawaban atas pertanyaan yang diinginkan dan kemudian pergi mengunjungi ke internet chat-room dan forum-forum diskusi yang membahas ketidaktahuan mereka. Kemungkinan pengguna yang terlihat oleh perekrut yang selalu mengawasi melalui forum-forum diskusi dan mendorong mereka kepada tahapan diskusi tentang isu-isu agama dan diskusi tentang sentimen politik dan kemudian melibatkan mereka kepada diskusi terorisme dan akhirnya indoktrinasi pribadi dalam perekrutan mereka.

- Komunikasi dan Jaringan

Kelompok-kelompok teroris baru-baru ini telah berubah dan memiliki hirarki yang jelas dalam organisasi dengan pemimpin yang ditunjuk, memiliki banyak pemimpin dan sel-sel pemimpin independen, sehingga pemimpin mereka dapat bersembunyi dengan aman. Internet memfasilitasi komunikasi antara sel-sel yang memungkin pertukaran informasi dan manual.

Internet juga membantu komunikasi internal didalam sel terutama dalam kaitannya dengan perencanaan serangan. Untuk menghindari dideteksi dan sebagai target oleh aparat keamanan, seringkali pesan dikirim oleh kelompok melalui email yang sangat populer seperti Hotmail dan Yahoo dan juga dapat dikirimkan dari tempat-tempat umum seperti perpustakaan dan internet cafe, kadang juga menggunakan chat-

room untuk memfasilitasi kegiatan mereka.

Selain itu, steganografi dapat digunakan untuk menyembunyikan informasi yang ditanam dalam file grafis disalah-satu situs web tersebut. File grafis juga dapat digunakan untuk mengirim pesan yang sangat halus seperti membalik orientasi pistol grafis yang artinya dapat saja sebagai rencana tahap berikutnya dan kelanjutan sebuah operasi. Metode lainnya untuk menyembunyikan petunjuk dan pesan dengan menggunakan bahasa kode

- Penggunaan disinformasi oleh kelompok-kelompok teroris sering digunakan untuk membangkitkan rasa takut dan panik kepada orang lain dengan mengirimkan berbagai ancaman ke korbannya seperti penayangan video eksekusi brutal, menciptakan serangan psikologis dsbnya melalui penggunaan ancaman cyberterorism.
- Disinformasi

  Cara ini digunakan untuk mengalihkan perhatian dari serangan balik dengan merilis berbagai serangan tipuan sehingga pemerintah dan aparat penegak hukum sulit untuk melacak mereka. Namun langkah-langkah ini tidak sepenuhnya efektif karena berlapisnya sistem keamanan saat ini sebagai contoh, setelah menerima informasi tentang potensi serangan (CERT Alert), tingkat keamanan pada semua spektrum diseluruh negara meningkat dari hitam, abu-abu dan akhirnya menjadi putih atau bebas dari ancaman cyber terrorism.

Seperti yang telah penulis sampaikan sebelumnya bahwa Di indonesia sendiri cyber terorisme di

atur dalam Undang-Undang Terorisme Nomor 1 Tahun 2002 , Undang-Undang ITE Nomor 19 Tahun 2016 dan peraturan Presiden Republik Indonesia Nomor 53 tahun 2017. Namun pokok perkara hukum yang sebenarnya bertumpu pada UU ITE No.19 tahun 2016 menurut hemat penulis masih banyak terdapat kelemahan yuridis dan dari formulasinya belum sistemik, karena memuat hal-hal yang bersifat umum dan belum mampu maksimal dalam menanggulangi jenis *cyber terorism* melalui sarana sistem hukum pidana dengan spesifik dan jelas, sehingga UU ITE No.19 tahun 2016 ini seringkali digunakan untuk menjerat pelaku yang semata-mata menggunakan sarana elektronik saja sehingga menimbulkan kesan ambigu dalam penerapannya karena menurut hemat penulis, seharusnya keberadaan UU ITE ini seharusnya lebih difokuskan kepada penanganan kejahatan dalam dunia siber yang didalamnya juga termasuk terorisme siber (*cyber terorism*).

Oleh karena itu penulis, dalam penelitian ini mengangkat judul Kebijakan Formulasi Hukum Pidana Tentang Penanggulangan Tindak Pidana Terorisme Siber (*Cyber Terorism*) Di Indonesia

D. Kesimpulan

Berdasarkan hasil penelitian awal, dapat disimpulkan bahwa kebijakan formulasi hukum terorisme siber (*cyber terorism*) termasuk didalamnya tentang pencegahan dan penanggulangan diantaranya telah ada dalam Undang-Undang Di indonesia sendiri cyber terorisme di atur dalam Undang-Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme yang telah

direvisi menjadi Undang undang No. 5 Tahun 2018 tentang Perubahan atas UU No 15 Tahun 2003 dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan untuk lembaga pendukung dan pihak terkait yang ikut serta dalam penanganan segalajenis tindak pidana dan serangan cyber di Indonesia di atur dalam Peraturan Presiden Republik Indonesia Nomor 53 tahun 2017 tentang Badan Siber dan Sandi Negara.

Namun undang-undang tersebut memiliki kelemahan yuridis yang mengakibatkan system pemidanaan tidak dapat berjalan dengan maksimal dan dapat menimbulkan ketidakpastian hukum, apalagi hingga mei 2021 belum terbentuk tim pengawas penanggulangan Terorisme. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elekronik juga belum mengatur secara jelas dan terperinci mengenai tindak pidana *cyber terrorism* seperti tidak menuangkan kata *cyber terrorism* atau terorisme siber sehingga dapat menimbulkan ketidakpastian hukum terhadap tindak pidana terorisme siber (*cyber terrorism*), selain itu, dasar pengenaan pasal untuk menjerat pelaku terorisme dengan menerapkan Undang-Undang No. 5 Tahun 2018 tentang Pemberantasan Tindak Pidana Terorisme atau pada Undang-Undang Nomor 19 Tahun 2016 tentang ITE, walaupun dapat digunakan, namun hanya sebatas pasal-pasal yang dapat mendukung atau cocok dengan satu sama

lainnya untuk dapat menjerat pelaku tindak pidana cyber terrorism akan tetapi dalam kedua undang-undang inI, karena tidak memberikan definisi gramatikal yang jelas mengenai *cyber* terrorism dapat menimbulkan ketidakpastian hukum atas Tindakan *cyber terrorism*, karena dalam tindak pidana terorisme Apabila dilihat dari skala aksi dan organisasinya, terorisme dibedakan antaraterorisme nasional, terorisme internasional, dan terorisme transnasional saja namun tidak memberikan definisi yang jelas tentang *cyber terrorism* / terorisme siber.

DAFTAR PUSTAKA

Buku

Edmon Makarim, 2005, Kompilasi Hukum Telematika, Jakarta, Raja Grafindo.

Golose, Petrus. 2015. Invasi Terorisme Ke Cyberspace. YPIK, Jakarta.

Maskun, 2013, Kejahatan Siber suatu pengantar, Jakarta, Prenada Media Grup

Suhariyanto Budi, Tindak Pidana Teknologi Informasi Cybercrime: Urgensi Pengaturan Dan Celah Hukumnya, Jakarta: Rajawali Pers, 2013.

Sunggono Bambang, 2015, Metodologi Penelitian Hukum Jakarta : Rajawali Pers

Suparni Niniek, 2009, Masalah Cyberspace : Problematika Hukum dan Antisipasi Pengaturannya, Jakarta : Fortun Mandiri Karya

Yonah Alexander, *Cyber Terorism and Information Welfare*, Oceana TM, United State

Zainuddin Ali, 2010, Metode Penelitian Hukum, Jakarta: Sinar Grafika, hlm.19

Jurnal dan Penelitian Lain

Arief, Barda N. 2005, Kebijakan Penanggulangan Cyber Crime dan Cyber Sex. Jurnal Law Reform,Vol. 1, No.1.

Goodall, K. 2013, Conceptualising ‘Racism’ in Criminal

Law. Cambridge University Legal StudieseeJournal,Vol. 33, No 2.

Sri Ayu Astuti, 2015, Penegakan Hukum Terhadap Terorisme Dunia Maya Di Indonesia, Jurnal Rechtsidee FH Universitas Muhamadiyah Sidoarjo.

Zahri Yunus dan Rabiah Ahmad, 2012, A Dynamic Cyber-terrorism Framework dalam Internasional Journal of Computer Science and Information Security Vo. 10, No 2.

Cyberterrorism and its prevention in Indonesia, Jurnal Media Hukum vol 27 no 2, 2020

Tindak pidana cyber terorism dalam transaksi elektronik, 2014 jurnal Lex administratum vol II no 3

Pengaturan Tindak Pidana Terorisme Dalam Dunia Maya (Cyber-Terrorism) Berdasarkan Hukum Internasional, jurnal kerthanegara 2016, vol 4 no 6

Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes, 2019, Jurnal Fiat Justisia, vol 13 no 4

Internet Dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism Melalui New Media 2017, jurnal gama societa.

Cyberterrorism: Suatu Tantangan Komunikasi Asimetris bagi Ketahanan Nasional, 2017, jurnal inter komunika, vol 2 no 1

Strategi Keamanan Cyber Security Di Kawasan Asia Tenggara: Self-Help Atau Multilateralism, 2019, Jurnal Asia Pacific Studies, Vol 3 No 2

Undang-Undang dan peraturan lainnya

Undang-undang Informasi dan Transaksi Elektronik No. 19 Tahun 2016

Media Online

Teuku Muhammad Radie, Makalah:Penelitian Hukum dalam Pembinaan dan Pembaharuan HukumNasional, 1974, Jakarta: BPHN Departemen Kehakiman, hlm. 14, online pada www.lib.ui.id/file?file=pdf/metadata-

20164472.pdf , diakses pada tanggal 25 Mei 2021

Dark web, https://cyberthreat.id/read/6226/Apa-Beda-Surface-Web-Deep-Web-dan-Dark-Web, akses 25 Mei 2021

pembentukan tim pengawas terorisme, https://www.dpr.go.id/berita/detail/id/32593/t/Legislator+Dorong+DPR+Segara+Bentuk+Tim+Pengawas+Penanggulangan+Terorisme, ases pada 25 mei 2021.

Ancaman teroris, https://inet.detik.com/cyberlife/d-1350189/7-ancaman-teroris-lewat-internet, akses 25 Mei 2021