**Jurnal Preferensi Hukum** | ISSN: XXXX | E-ISSN: XXXX
Vol. 1, No. 2 – September 2020, Hal. 21-27| Available Online at https://www.ejournal.warmadewa.ac.id/index.php/juprehum
DOI: http://doi.org/10.22225/jph.v1i2.2337.21-27

# KEBIJAKAN HUKUM PIDANA BAGI TINDAK PIDANA *CYBER TERRORISM* DALAM RANGKA PEMBENTUKAN HUKUM POSITIF DI INDONESIA

Zephirinus Jondong
Fakultas Ilmu Hukum Universitas Warmadewa, Denpasar – Bali, Indonesia

**Abstrak**

Kemajuan teknologi komputer berbasis internet tidak hanya memberikan dampak positif saja kepada penggunanya, tetapi juga memberikan dampak negatif, salah satunya adalah terciptanya bentuk-bentuk kejahatan baru seperti kejahatan terorisme. Berdasarkan latar belakang tersebut, penelitian ini dilakukan dengan tujuan mengungkap bagaimana pengaturan tindak pidana terorisme yang dilakukan melalui dunia maya (cyber terrorism) dalam hukum positif di Indonesia dan bagaimana kebijakan hukum pidana di Indonesia pada masa yang akan datang dalam hal pengaturan tindak pidana terorisme yang dilakukan melalui dunia maya (cyber terrorism). Penelitian ini didesain menggunakan metode penelitian hukum normatif. Hasil penelitian ini mengungkap bahwa di Indonesia tindak pidana *cyber terrorism* tidak diatur di dalam Kitab Undang- Undang Hukum Pidana (KUHP) maupun Peraturan Perundang-Undangan yang mengatur di bidang terorisme. Dalam situasi seperti ini, pelaku tindak pidana *cyber terrorism* dapat dinyatakan bebas dari pidana karena tidak terdapat unsur melawan hukum yang diatur dalam Undang-Undang melekat pada perbuatannya tersebut. Oleh karena itu, untuk dapat dijatuhi suatu pidana, maka tindak pidana cyber terrorism harus dirumuskan secara tegas dan jelas. Selain itu, dalam membentuk kebijakan hukum pidana mengenai tindak pidana *cyber terrorism*, perbuatan *cyber terrorism* harus diperhatikan dan dipertimbangkan agar dapat dijadikan tindak pidana dan sanksi dapat dijatuhkan kepada pelaku.

**Kata kunci:** *Cyber Terrorism*; Hukum Positif; Kebijakan Hukum Pidana

***Abstract***

*The advancement of internet-based computer technology has not only a positive impact on its users but also a negative impact, one of which is the creation of new forms of crime such as terrorism. Based on this background, this research was conducted with the aim of revealing how the regulation of criminal acts of terrorism committed through cyberspace (cyber terrorism) in positive law in Indonesia and how criminal law policies in Indonesia in the future in regulating criminal acts of terrorism committed through cyberspace (cyber terrorism). This research was designed using normative legal research methods. The results of this study reveal that in Indonesia, the criminal act of cyber terrorism is not regulated in the Criminal Code (KUHP) or the Laws and Regulations that regulate the field of terrorism. In a situation like this, the perpetrator of the crime of cyber terrorism can be declared free from punishment because there is no element against the law regulated in the Act attached to the act. Therefore, in order to be convicted of a crime, the crime of cyber terrorism must be formulated clearly. In addition, in establishing a criminal law policy regarding cyber terrorism, cyber terrorism must be considered so that it can be made a criminal act and sanctions can be imposed on the perpetrator.*

***Keywords:*** *Cyber Terrorism; Positive Law; Criminal Law Policy*

## I. PENDAHULUAN

Indonesia adalah Negara Hukum yang mempunyai kewajiban dalam memberikan perlindungan kepada setiap warga Negara dari tindakan kejahatan. Upaya untuk menciptakan peraturan perundang-undangan yang sesuai dengan tujuan hukum itu sendiri adalah melalui penegakan hukum. Upaya ini diwujudkan pemerintah dengan mengeluarkan perpu No.1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme yang merupakan suatu kejahatan luar biasa sehingga membutuhkan penanganan yang luar biasa juga.

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 di dunia maya karena cakupan dan muatan pengaturan dalam dunia maya yang begitu luas.

Saat ini *cyber terrorism* telah menjadi isu besar di setiap negara (Sarinastiti & Vardhani, 2018; Ufran, 2014). Oleh karena itu, perlu dilakukan dengan segera sebuah tindakan antisipasi berupa pembaharuan hukum pidana atau kebijakan hukum 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 (Sudarto, 1983).

Kebijakan hukum pidana dalam tujuannya untuk menegakkan hukum dan menanggulangi tindak pidana *cyber terrorism* 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 No. 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi sebuah Undang-undang (yang selanjutnya disingkat menjadi UU Terorisme) jo.

Berdasarkan latar belakang yang telah diuraikan di atas, penelitian ini dilakukan dengan tujuan mendeskripsikan baagaimana pengaturan tindak pidana terorisme yang dilakukan melalui dunia maya (cyber terrorism) dalam hukum positif di Indonesia dan bagaimana kebijakan hukum pidana di Indonesia pada masa yang akan datang dalam hal pengaturan tindak pidana terorisme yang dilakukan melalui dunia maya (cyber terrorism).

## II. METODE PENELITIAN

Penelitian ini didesain dengan menggunakan metode penelitian hukum normatif. Penelitian ini menguraikan permasalahan-permasalahan yang ada dengan mengkaji berdasarkan teori-teori hukum yang dikaitkan dengan Peraturan Perundang-Undangan yang berlaku dalam praktek hukum. Penelitian ini diawali dengan adanya suatu persoalan dalam norma hukum, yakni adanya kekosongan hukum dalam Peraturan Perundang-Undangan yang hendak diteliti. Penelitian hukum normatif tersebut berusaha untuk mengkaji dan mendalami serta mencari jawaban tentang apa yang seharusnya dari setiap permasalahan (Marzuki, 2011). Tipe pendekatan dalam penelitian ini dilakukan melalui pendekatan perundang-undangan (statute approach), pendekatan analisis konsep hukum (analitical & conseptual approach), pendekatan perbandingan (comparative approach), dan pendekatan kasus (the case approach). Sumber data penelitian ini adalah Uundang-Undang yang berkaitan dengan pencegahan dan pemberantasan terorisme dan kajian-kajian sebelumnya tentang terorisme, dan pendapat para ahli hukum. Data-data yang dibutuhkan dalam penelitian ini dikumpulkan dengan menggunakan metode kajian pustaka. Data yang tekumpul dianalisis menggunakan metode kualitatif dan disajikan secara deskriptif.

## III. HASIL DAN PEMBAHASAN

### *1. Pengaturan Tindak Pidana Terorisme yang Dilakukan melalui Dunia Maya (Cyber Terrorism) dalam Hukum Positif di Indonesia*

*Cyberspace* 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 (Astuti, 2015; Lubis, 2017). 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 *cybercrime* sebagaimana yang telah diuraikan sebelumnya, namun satu hal yang harus dipahami bahwa sesuai dengan pendapat Denning (2000), *cyber terrorism* merupakan konvergensi dari *cyberspace* dan terorisme. Oleh karena itu, unsur terorisme dalam *cyber terrorism* juga harus diperhatikan karena kejahatan terorisme memiliki motif tersendiri.

Di Indonesia, tindak pidana *cyber terrorism* tidak diatur di dalam Kitab Undang-Undang Hukum Pidana (KUHP) maupun peraturan perundang-undangan yang mengatur di bidang terorisme, terutama dalam Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Perpu No 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-undang jo. Penetapan Perpu No.1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme serta Undang- undang RI No. 9 Tahun 2013 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme.

Hal tersebut mengakibatkan adanya kekosongan hukum yang mengatur mengenai tindak pidana *cyber terrorism* yang dibuktikan melalui analisa ketentuan hukum yang ada dan berlaku di Indonesia. Karakteristik pertama *cyber terrorism* adalah tindakan teror terhadap sistem komputer, jaringan, dan/ atau basis dan informasi yang tersimpan dalam komputer. Adapun bentuk-bentuk perbuatan yang termasuk kategori ini antara lain:

a. *Unauthorized access to computer system and service*, yaitu kejahatan menggunakan system komputer melalui jaringan secara tidak benar dan tanpa ijin dari pemilik.
b. *Denial of service attack* (DoS), yakni menyerang dengan cara memenuhi jaringan dengan permohonan dalam hitungan detik untuk mendapatkan layanan data sehingga mengakibatkan jaringan bekerja terlalu keras, atau mati, atau melambatnya kinerja jaringan.
c. *Cyber sabotage and extortion*, yaitu kejahatan yang dilakukan dengan menggangu, merusak, atau menghancurkan suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet.
d. *Viruses*, yakni kejahatan yang dilakukan dengan menyebarkan perangkat lunak seperti program, script, atau macro yang telah dirancang untuk menginfeksi, menghancurkan, memodifikasi, dan menimbulkan masalah terhadap komputer atau program komputer.
e. *Physical attacks*, yakni penyerangan fisik yang dilakukan terhadap sistem komputer atau jaringan komputer, dengan cara-cara pembakaran, pencabutan salah satu device komputer atau jaringan yang menyebabkan lumpuhnya sistem komputer.

Beberapa dari kelima perbuatan di atas, jika dikaji merupakan bagian dari perbuatan-perbuatan yang dilarang dalam UU ITE, seperti yang diuraikan di bawah ini:

a. Pasal 30 UU ITE mengatur tentang tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun. Konstruksi perbuatan dalam rumusan pasal ini menjelaskan bahwa tindakan tidak sah/illegal yang dilakukan oleh seseorang terhadap sistem elektronik milik orang lain dengan tujuan untuk memproleh informasi/dokumen elektronik dan/atau upaya pembobolan, penerobosan, dan penjebolan yang melanggar dan melampaui sistem pengamanan.
b. Pasal 32 dan Pasal 33 UU ITE yang mengatur tentang perlindungan terhadap suatu informasi dan/atau dokumen elektronik baik milik orang lain atau milik publik yang bersifat rahasia.

Sifat melawan hukum dalam Pasal 30 UU ITE tersebut memiliki dua corak, yakni melawan hukum objektif dan melawan hukum subjektif. Melawan hukum objektif berarti komputer dan/ atau sistem komputer tersebut bukan milik pelaku dan perbuatan mengakses komputer dan/ atau sistem elektronik tersebut tanpa izin pemilik/ tanpa hak.

Sama halnya dengan Pasal 30 UU ITE, Pasal 32 UU ITE juga memiliki dua corak sifat melawan hukum. Sifat melawan hukum yang objektif dalam rumusan pasal ini terdapat pada unsur objeknya, bahwa Informasi Elektronik dan/ atau Dokumen Elektronik tersebut milik orang lain. Agar rumusan tersebut memenuhi sifat melawan hukum yang objektif, maka frasa milik orang lain tersebut harus dibuktikan dan dipastikan keberadaannya melalui perbuatan mengubah dan sebagainya tersebut harus tidak ada izin dari pemiliknya.

Sedangkan sifat melawan hukum yang subjektifnya terletak pada keadaan batin si pelaku terhadap sifat melawan hukum objektifnya perbuatan. Pelaku mengetahui bahwa perbuatan Yang hendak diperbuatnya adalah yang mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, serta memindahkan,dan menyembunyikan dengan cara apapun suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik sebagai perbuatan yang tercela (Chazawi & Ferdian, 2011).

Sifat melawan hukum dalam Pasal 33 UU ITE terletak pada akibat perbuatan tersebut, yakni perbuatan pelaku tersebut akan mengakibatkan terganggunya atau tidak bekerjanya sistem elektronik tersebut sebagaimana mestinya.

Pasal 30, Pasal 32, dan Pasal 33 UU ITE pada dasarnya ditargetkan untuk mempidana pelaku terorisme cyber. Sebagai catatan, dalam perkembangannya, muncul dua istilah yang semakin sulit untuk dibedakan, yakni munculnya istilah *cyber terrorism* dan terorisme siber (pelaku cyber crime). Cyber terrorism menurut Denning (2000) adalah perbuatan melawan hukum yang dilakukan dengan menyerang komputer, jaringan, dan informasi yang tersimpan di dalamnya serta bertujuan untuk mengintimidasi atau memaksa pemerintah atau masyarakat untuk tujuan politik dan sosial atau jika penulis artikan secara singkat adalah terorisme yang dilakukan melalui dunia maya atau teroris yang menggunakan teknologi siber, sedangkan terorisme siber adalah perbuatan seseorang atau beberapa orang yang bertujuan untuk melakukan serangan siber. Prinsip anonimitas menjadi faktor yang menjadikan perbedaan antara istilah tersebut semakin menghilang (Garadian, 2017).

Terorisme siber cenderung tidak mempunyai anggota kelompok dalam jumlah besar, sedangkan terorisme yang menggunakan dunia maya mempunyai banyak anggota bahkan cabang yang tersebar di seluruh dunia. Serangan yang dilakukan atas dasar terorisme siber tidak diafiliasi dengan kelompok teroris manapun di seluruh dunia, meskipun terdapat motif politik di dalamnya (Garadian, 2017). Sedangkan, terorisme yang menggunakan dunia maya adalah terorisme yang memanfaatkan kemajuan teknologi dan informasi sebagai media untuk melakukan aktivitas 9P mereka, yaitu propaganda, perekrutan, penyediaan logistik, pelatihan, pembentukan para militer melawan hukum, perencanaan, pelaksanaan serangan teroris, persembunyian, dan pendanaan.

Relevansi Pasal 30, Pasal 32, dan Pasal 33 UU ITE dengan perbuatan tindak pidana *cyber terrorism* adalah bentuk perbuatan akses tidak sah atau gangguan terhadap data komputer, informasi/ dokumen elektronik milik orang lain atau milik publik yang dilakukan dengan cara pembobolan, penerobosan, dan penjebolan yang melanggar, melampaui sistem pengamanan, dan sebagainya yang memenuhi unsur cara-cara melakukan teror dalam tindak pidana *cyber terrorism*.

Namun, sifat melawan hukum untuk tindak pidana *cyber terrorism* tidak terpenuhi dalam rumusan pasal-pasal UU ITE karena dalam tindak pidana *cyber terrorism* serangan atau ancaman secara melawan hukum tersebut dilakukan 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.

Sebagaimana terorisme yang dilakukan secara konvensional yang mengakibatkan kerusakan umum atau suasana teror atau rasa takut terhadap orang secara meluas. Sama halnya dengan unsur akibat serangan dalam terorisme konvensional, bahwa suatu tindakan dapat dikategorikan sebagai *cyber terrorism* apabila serangan tersebut menciptakan ketakutan dan mengakibatkan korban pada daerah sekitarnya atau secara meluas, meskipun bukan target utama dari serangan mereka. Hal tersebut menjadikan kekosongan hukum dalam pengaturan UU ITE untuk menanggulangi tindak pidana *cyber terrorism*.

Selanjutnya, karakteristik kedua, yakni *cyber terrorism* sebagai pemanfaatan internet oleh para teroris untuk keperluan organisasi dan media teror kepada pemerintah dan masyarakat, dapat digali dan dianalisa pengaturannya dalam UU Pemberantasan Tindak Pidana Terorisme, sebagaimana rumusan dalam Pasal 6 UU Pemberantasan Tindak Pidana Terorisme.

Pertanggungjawaban pidana merupakan suatu terusan celaan bagi pelaku atas tindak pidana yang telah dilakukannya. Celaan dalam pertanggungjawaban pidana dibagi atas celaan secara objektif dan celaan secara subjektif. Celaan secara objektif berarti pelaku telah melakukan tindak pidana (perbuatan yang dilarang atau melawan hukum dan dapat diberi pidana berdasarkan hukum yang berlaku atau asas legalitas), sedangkan celaan secara subjektif berarti pelaku patut untuk dicela atau diminta pertanggungjawabannya atas tindak pidana yang telah dilakukannya.

*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 situasi seperti ini, pelaku tindak pidana cyber terrorism dapat dinyatakan bebas dari pidana karena tidak terdapat unsur melawan hukum yang diatur dalam Undang-Undang 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.

### *2. Kebijakan Hukum Pidana di Indonesia pada Masa yang akan Datang dalam Hal Pengaturan Tindak Pidana Terorisme yang Dilakukan melalui Dunia Maya (Cyber Terrorism)*

Usaha penanggulangan kejahatan melalui hukum pidana merupakan bagian dari usaha penegakan hukum, khususnya bagi penegakan dalam bidang hukum pidana. Oleh karena itu, politik atau kebijakan hukum pidana merupakan bagian dari kebijakan penegakan hukum (Arief, 2014: 23). Kemudian, dalam rangka membentuk kebijakan hukum pidana tersebut, diperlukan suatu pembaharuan dalam bidang hukum pidana.

Sebagaimana telah diuraikan sebelumnya bahwa pembaharuan hukum pidana pada hakikatnya adalah suatu upaya untuk melakukan reorientasi dan reformasi hukum pidana yang sesuai dengan nilai-nilai sentral sosio-politik, sosio-filosofis, dan sosio kultural masyarakat Indonesia yang melandasi kebijakan kriminal dan kebijakan penegakan hukum Indonesia (Arief, 2014: 31). Pembaharuan hukum pidana tersebutlah yang harus dilakukan melalui pendekatan kebijakan.

Fenomena berkembangnya bentuk tindak pidana terorisme konvensional menjadi tindak pidana terorisme yang menggunakan internet membuat badan legislatif harus dengan segera membentuk suatu kebijakan hukum pidana mengenai tindak pidana *cyber terrorism*. Meskipun Indonesia telah memiliki UU ITE yang mengatur tentang kejahatan di bidang komputer namun Undang-Undang tersebut dianggap tidak mampu untuk menanggulangi tindak pidana *cyber terrorism*. Hal tersebut dikarenakan UU ITE hanya mengarah ke bentuk *cyber terrorism*, tetapi UU ITE tidak mengatur secara materiil mengenai ketentuan penegakan hukum bagi tindak pidana *cyber terrorism*.

Dalam membentuk kebijakan hukum pidana mengenai tindak pidana *cyber terrorism*, maka harus diperhatikan mengenai perbuatan *cyber terrorism* yang bagaimana agar dapat dijadikan tindak pidana dan sanksi yang dijatuhkan kepada pelaku. Hal ini ditujukan agar kebijakan hukum pidana yang baru ini mampu menjangkau delik cyber terrorism di masa depan, sehingga harus dipersiapkan secara matang melalui pendekatan yang berorientasi pada kebijakan (policy oriented approach) dan pendekatan yang berorientasi pada kebijakan nilai (value oriented approach).

Berdasarkan uraian tersebut, maka faktor yang harus diperhatikan dalam perumusan perbuatan *cyber terrorism* agar dapat dijadikan tindak pidana antara lain:

1) Komputer merupakan salah satu teknologi yang sangat strategis bagi pembangunan nasional serta kemajuan suatu bangsa dan negara. Oleh karena itu, kebijakan yang dibentuk jangan sampai menimbulkan efek samping yang dapat menghambat pengembangan teknolog ikomputer,pengaplikasiannya, dan perkembangan dalam industri komputer yang ditujukan bagi kemajuan bangsa dan negara.
2) Berkaitan dengan butir 1, pemilihan dan penetapan perbuatan cyber terrorism ke dalam suatu delik harus dilakukan secara selektif dan limitatif. Delik tersebut harus benar-benar perbuatan yang sangat tidak dikehendaki, tidak disukai, atau dibenci oleh seluruh masyarakat, yakni perbuatan yang merugikan secara materiil maupun spiritual, atau perbuatan yang dapat menghasilkan korban, serta perbuatan yang sangat bertentangan dengan nilai-nilai fundamental dalam masyarakat.

3) Memperhatikan biaya (cost) dalam pembuatan Undang-Undang agar disesuaikan dengan biaya untuk pengawasan dan penegakan hukum.
4) Memperhatikan kapasitas atau kemampuan penegak hukum di Indonesia secara kualitas dan kuantitas.
5) Memperhatikan akibat sosial dari kriminalisasi atau pendeskriminalisasian tindak pidana *cyber terrorism* terhadap masyarakat (Wisnubroto, 1999). Sedangkan, faktor-faktor yang harus diperhatikan dalam penetapan sanksi pidana terhadap tindak pidana *cyber terrorism*, antara lain:
    a) Pemeliharaan tertib masyarakat dan perlindungan masyarakat dari kejahatan, kerugian, atau bahaya-bahaya yang tidak dapat dibenarkan.
    b) Memasyarakatkan kembali (resosialiasi) para pelaku.
    c) Memelilhara atau mempertahankan integritas pandangan dasar tertentu mengenai keadilan sosial, martabat kemanusiaan, dan keadilan individu (Wisnubroto, 1999).

## IV. SIMPULAN DAN SARAN

### *1. Simpulan*

Berdasarkan hasil dan pembahasan yang telah diuraikan di atas, ada beberapa simpulan yang dapat dibuat, yaitu: pertama, pengaturan tentang kejahatan *cyber terrorism* tidak diatur dalam berbagai hukum positif di Indonesia, baik dalam undang-undang yang mengatur tentang *cyber law* (seperti UU ITE) dan Undang-Undang yang mengatur tentang terorisme (seperti UU Pemberantasan Tindak Pidana Terorisme dan UU Pendanaan 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. Pertanggungjawaban pidana hanya dapat dilakukan terhadap seseorang yang melakukan tindak pidana. Kedua, dalam membentuk kebijakan hukum pidana mengenai tindak pidana *cyber terrorism*, perbuatan *cyber terrorism* harus diperhatikan dan dipertimbangkan agar dapat dijadikan tindak pidana dan sanksi dapat dijatuhkan kepada pelaku.

### *2. Saran*

Berdasarkan hasil dan pembahasan penelitian ini, ada beberapa saran kepada beberapa pihak, yaitu: pertama, kepada badan legislatif 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 hukum atas bentuk-bentuk kejahatan *cyber terrorism* yang mengancam keamanan setiap orang dan negara serta dapat mewujudkan kodifikasi hukum pidana nasional. Kedua, 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

Astuti, S. A. (2015). Penegakan Hukum terhadap Terorisme Dunia Maya di Indonesia. *Rechtsidee*, *2*(2), 1–19.

Chazawi, A., & Ferdian, A. (2011). *Tindak Pidana Informasi dan Transaksi Elektronik: Penyerangan terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*. Malang: Bayumedia Publishing.

Denning, D. E. (2000). *Cyberterrorism*.

Garadian, E. A. (2017). *Terorisme dan Dunia Virtual* (J. Jahroni & J. Makruf, eds.). Retrieved from

Lubis, R. R. (2017). Potensi Pengguna Internet Indonesia dalam Counter-Cyber Radicalization. *Jurnal Pertahanan & Bela Negara*, *7*(2), 19–34.

Marzuki, P. M. (2011). *Penelitian Hukum* (11th ed.).

Sarinastiti, E. N., & Vardhani, N. K. (2018). Internet dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism melalui New Media. *Jurnal Gama Societa*, *1*(1), 40–52.

Sudarto. (1983). *Hukum Pidana dan Perkembangan Masyarakat*.

Ufran. (2014). Kebijakan Antisipatif Hukum Pidana untuk Penanggulangan Cyberterrorism.

*Kebijakan Antisipatif Hukum Pidana Untuk Penanggulangan Cyberterrorism*, *43*(4), 529–537.
Wisnubroto, A. (1999). *Kebijakan Hukum Pidana dalam Penanggulangan Penyalahgunaan Komputer*.